Burnett Business Centre
accounting tax and financial services
it's all about you

67 Fitzroy Street
PO Box 130
Nanango Qld 4615
Ph: 07 4160 9000
E: team@bbuscentre.com.au
www.bbuscentre.com.au

Privacy Policy

When you trust us with your personal information, you expect us to protect it and keep it safe.

We are bound by the *Privacy Act 1988* (Cth) (**Privacy Act**) and will protect your personal information in accordance with the *Australian Privacy Principles* (**APPs**). These principles govern how we can collect, use, hold and disclose your personal information, as well as ensuring the quality and security of your personal information.

The defined terms in this Policy have the same meaning as detailed in our 'Letter of Engagement', which you should read together with this Policy. By using our services, you consent to the terms of this Policy and agree to be bound by it and our terms of engagement.

If you would like more information about how we protect your privacy, please contact us.

About this policy

This privacy policy explains how we manage your personal information. We may provide more details on how we manage your personal information when we collect your personal information.

This policy applies to any person for whom we currently hold, or may in the future collect, personal information.

What information does the privacy policy apply to?

This policy applies to personal information. In broad terms, 'personal information' is information or opinions relating to a particular individual who can be identified.

Information is not personal information where the information cannot be linked to an identifiable individual.

The information that we seek to collect about you will depend on the nature of our interaction with you. If you do not allow us to collect all of the information we request, we may not be able to interact with you.

What kinds of personal information do we collect and hold?

We are a full-service accountancy and financial planning firm and hold different information depending on the nature of our interaction with you. Generally, the types of information that we may collect and hold about our current and prospective clients (or individual representatives of, or individuals otherwise involved with, such) includes:

- sensitive information (see below)
- contact information;
- financial information;
- business circumstances;

- family circumstances;
- information about assets and investments;
- employment history;
- date and place of birth;
- insurance history;
- insurance information;
- banking and credit card details;
- credit information
- expertise and interests;
- tax file numbers and tax returns;
- government related identifiers;
- driver's licence and other photographic information;
- information otherwise required by law; and
- any other personal information required to perform the financial or accounting service to the individual.

Where possible, we will only collect the personal information required to provide the accountancy and/or financial planning service to the individual, or as required by our professional obligations.

For example, when you apply for our products or services we may ask for identification information. If you apply for insurance, we may collect information about what is being insured, the beneficiaries, and your health and financial situation, depending on the type of insurance.

Throughout the life of your product or service, we may collect and hold additional personal information about you. This could include transaction information or making a record of queries or complaints you make and, if you make an insurance claim, collecting additional information to assess the claim.

If you are a current or prospective contractor, consultant or agent or prospective employee we may collect and hold personal information including:

- sensitive information (see below);
- contact information;
- date of birth;
- employment history;
- tax file number information;
- government related identifiers;
- insurance information and claims history;
- credit information;
- licence details;
- education details;
- driving history;
- banking details;
- any other personal information required to engage you as our contractor, consultant, agent or employee; and
- records of contact and details of enquiries, conversations or correspondence made or received from you.

Sensitive Information

The collection of sensitive information is restricted by the Privacy Act. Sensitive information is a subset of personal information and includes personal information that may have serious ramifications for the individual concerned if used inappropriately.

The sensitive information we collect and hold about current and prospective clients may include health information or biometric information.

It is more likely that we would collect sensitive information from our current or prospective contractors, consultants or agents or our prospective employees such as:

- health information;
- criminal records;
- membership of professional or trade associations;
- membership of trade unions; and

Generally, we only collect this sort of information if it is necessary to provide you with a specific product or service (or in the case of prospective or current contractors, consultants or agents or our prospective employees, to employ or engage you) and you have consented to that collection. For example, we may collect health information about you to process a claim under an insurance policy or collect voice biometric information to verify your identity or authorise transactions.

We will not collect sensitive information without the individual's consent to whom the information relates unless permitted under the Privacy Act.

For what purposes do we collect, hold, use and disclose personal information?

We take reasonable steps to use and disclose personal information for the primary purpose for which we collect it. The primary purpose for which information is collected varies, depending on the individual that we are collecting information from but is generally as follows:

- in the case or current or prospective clients, to provide our products and services;
- in the case of current contractors, consultants or agents, to assist us in providing our products and services; and
- in the case of prospective contractors, consultants, agents or employees, to assess suitability for employment or engagement with us.

Personal information may also be used or disclosed by us for secondary purposes that are within your reasonable expectations and that are related to the primary purpose of collection.

For example, we may collect and use your personal information to:

- to keep records of transactions to assist in future enquiries;
- enhance our relationship with you;
- verify your identity;
- check whether you are eligible for the product or service;

- assist you where online applications are not completed;
- provide a product or service;
- help manage a product or service;
- refer you to other advisers;
- provide you with updates and alerts that are relevant to you and your business; and
- invite you to events.

We may also use your information to comply with legislative or regulatory requirements in any jurisdiction, prevent fraud, crime or other activity that may cause harm in relation to our products or services and to help us run our business.

How do we collect personal information?

Our usual approach to collecting personal information is to collect it directly from you.

We may collect personal information directly from you when you:

- Agree to engage us to use our services,
- use the services,
- complete documentation requirements – fill in Forms and provide us information about yourself,
- contact us; and
- visit our Website.

We also collect information from you electronically. For instance, when you visit our website or if you send us electronic correspondence (see "Do we collect personal information electronically?").

Sometimes we collect personal information about you from other people or organisations. This may happen without your direct involvement. For instance, we may collect personal information about you from:

- publicly available sources of information, such as public registers;
- your representatives (including your legal adviser, mortgage or insurance broker, executor, administrator, guardian, trustee, or attorney);
- banks and financial institutions;
- government bodies;
- businesses about their employees, contractors, customers or suppliers;
- your employer;
- feedback surveys;
- other organisations, who jointly with us, provide products or services to you;
- through marketing and business development activities;
- commercial information service providers, such as companies that provide fraud prevention reports and paid search providers; and
- insurers, re-insurers and health care providers.

We may receive personal information from you about other family members or related parties.

Through your use of our services we may also collect information from you about someone else. If you provide us with personal information about someone else, you must ensure that you are authorised to disclose that information to us and that, without us taking any further steps required by applicable data protection or privacy laws, we may collect, use and disclose such information for the purposes described in this Policy.

This means that you must take reasonable steps to ensure the individual concerned is aware of and/or consents to the various matters detailed in this Policy, including the fact that their personal information is being collected, the purposes for which that information is being collected, the intended recipients of that information, the individual's right to obtain access to that information, our location and identity and how to contact us.

Where requested to do so by us, you must also assist us with any requests by the individual to access or update the personal information you have collected from them and entered into the Service.

What laws require or authorise us to collect personal information?

We are required or authorised to collect:

- certain identification information about you by the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) and *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)*;
- your Tax File Number, if you choose to provide it, by the *Income Tax Assessment Act 1936* (Cth); and
- certain information in relation to your application if you have applied for an insurance as required by the *Insurance Contracts Act 1984* (Cth).

How do we hold and manage personal information?

We are committed to protecting the security of your personal information and we take all reasonable precautions to protect it from unauthorised access, modification or disclosure. Your personal information is stored at our offices, on our servers and our website that have restricted and limited access both physically and virtually.

Much of the information we hold about you will be stored electronically in data centres and private clouds. Some information we hold about you will be stored in paper files. We use a range of physical and electronic security measures to protect the security of the personal information we hold. For example:

- access to information systems is controlled through identity and access management;
- employees are bound by internal information security policies and are required to keep information secure;
- all employees are required to complete training about information security; and
- we regularly monitor and review our compliance with internal policies and industry best practice.

Subject to our professional obligations, we take reasonable steps to destroy or permanently de-identify any personal information after it can no longer be used.

In limited circumstances, it may be possible for you to use a pseudonym or remain anonymous when dealing with us. If you wish to use a pseudonym or remain anonymous you should notify us when making first enquiries or providing initial instructions. We will use our best endeavours to deal with your request, subject to our professional obligations and ability to perform the accounting service to you without using your name. In most cases, our professional obligations will require you to deal with us using your real name.

We are also subject to professional obligations that may affect how we deal with personal information.

We manage the personal information we collect in numerous ways, such as by:

- implementing procedures for identifying and managing privacy risks at each stage of the information lifecycle, including collection, use, disclosure, storage, destruction or de-identification;
- implementing security systems for protecting personal information from misuse, interference and loss from unauthorised access, modification or disclosure;
- regularly providing staff with training on privacy issues;
- appropriately supervising staff who regularly handle personal information;
- implementing mechanisms to ensure any agents or contractors who deal with us comply with the APPs;
- implementing procedures for identifying and reporting privacy breaches and for receiving and responding to complaints;
- appointing a privacy officer within the business to monitor privacy compliance.
- having access to audit trails of information accessed; and
- allowing individuals the option of not identifying themselves, or using a pseudonym, when dealing with us in particular circumstances.

The Internet is not in itself a secure environment and we cannot give an absolute assurance that your information will be secure at all times. Transmission of personal information over the Internet is at your own risk and you should only enter, or instruct the entering of, personal information to our office within a secure environment.

We will advise you at the first reasonable opportunity upon discovering or being advised of a security breach where your personal information is lost, stolen, accessed, used, disclosed, copied, modified, or disposed of by any unauthorised persons or in any unauthorised manner.

Who do we disclose your personal information to?

In the course of our business, we may disclose personal information to:

- our agents, contractors and external service providers (for example mailing houses and technology service providers);
- paraplanning service providers;
- insurers, re-insurers and health care providers;
- payment systems operators (for example, merchants receiving card payments);

- other organisations, who jointly with us, provide products or services to you;
- financial services organisations, including banks, superannuation funds, stockbrokers, custodians, fund managers and portfolio service providers;
- debt collectors;
- legal advisers or auditors;
- your representatives (including your legal adviser, accountant, mortgage broker, executor, administrator, guardian, trustee, or attorney);
- fraud bureaus or other organisations to identify, investigate or prevent fraud or other misconduct;
- IT Service Providers;
- Our Licensee, Sentry Financial Services Pty Ltd ABN 30 113 531 034 (AFSL 286786) and its related entities;
- external dispute resolution schemes;
- superannuation clearing houses; and
- regulatory bodies, government agencies and law enforcement bodies in any jurisdiction (including the Australian Taxation Office).

We may also disclose your personal information to third parties where:

- we are required or authorised by law or where we have a public duty to do so;
- you may have expressly consented to the disclosure or the consent may be reasonably inferred from the circumstances; or
- we are otherwise permitted to disclose the information under the Privacy Act.

Do we disclose personal information overseas?

We may disclose your personal information to a recipient which is located outside Australia. This includes:

- Our outsourced service providers or employees that may be located in the Philippines.
- Any financial institution which you hold an account with overseas where you have given us permission to make enquiries on your behalf.
- Disclosure of information through the use of a cloud or other outsourced information technology services. For example, we may choose to use software providers which store data on overseas servers, such as:
- Microsoft Azure server & virtual desktop services on servers all located in Australia.
- Microsoft 365 which we understand predominately stores information in Australia and the United States of America, as well as potentially Austria, Brazil, Canada, Chile, Finland, France, Germany, Hong Kong, India, Ireland, Japan, Korea, Luxembourg, Malaysia, the Netherlands, Singapore, South Africa, and the United Kingdom.
- MYOB AE Desktop, MYOB Practice, and MYOB Client software that utilise Microsoft Azure and Amazon Web Services that store data on servers in Australia
- MYP that stores data on servers located in Australia.
- QuickBooks Online, Xero, Common Ledger, Employment Hero and others that use Amazon Web Services (AWS), which we understand stores data on servers in Australia as well as the United States of America, Ireland, Canada, Europe, Brazil, Singapore and Japan;

- Teamviewer, which we understand predominantly stores information in Germany but also in the United States of America &the EU / European Economic Area (EEA).
- Zoom, which we are able to set most features to use data centres based in Australia, but that also stores data in the United States, as well as in other countries outside of the EEA, Switzerland, and the UK.
- Xplan/Iress which we understand stores information in Australia, as well as the United Kingdom, Singapore, Malaysia, Tunisia, Hong Kong, South Africa, New Zealand, the United State of America (USA), and Canada
- Other software that we understand do not store data on overseas servers, such as BGL 360, (AWS Australia), Reckon (AWS Australia), ATO Smartdocs / ipracticeapp (Azure in Australia), Cash Flow Story, and others.

Your personal information will not be disclosed to overseas recipients unless we are satisfied that the recipient is subject to privacy protection laws that offer substantially similar levels of protection as those required under the APPs or if we have taken reasonable steps to ensure this personal information is handled in a safe and secure manner and that overseas entity is aware of the obligations relating to the information under the APPs.

Do we use or disclose personal information for marketing?

We will use your personal information to offer you products and services we believe may interest you, but we will not do so if you tell us not to. We may offer you products and services by various means, including by mail, telephone, email, SMS or other electronic means, such as through social media or targeted advertising through our website.

We may also disclose your personal information to third party organisations who assist us to market our products and services to you.

If you don't want to receive marketing offers from us please contact us.

Do we collect personal information electronically?

We will collect information from you electronically, for instance through internet browsing, mobile or tablet applications.

Each time you visit our website, we collect information about your use of the website, which may include the following:

- The date and time of visits;
- Which pages are viewed;
- How users navigate through the site and interact with pages (including fields completed in forms and applications completed);
- Location information about users;
- Information about the device used to visit our website; and
- IP addresses.

We use technology called cookies when you visit our site. Cookies are small pieces of information stored on your hard drive or in memory. They can record information about your visit to the site, allowing it to remember you the next time you visit and provide a more meaningful experience.

One of the reasons for using cookies is to offer you increased security. The cookies we send to your computer cannot read your hard drive, obtain any information from your browser or command your computer to perform any action. They are designed so that they cannot be sent to another site, or be retrieved by third party sites.

We won't ask you to supply personal information publicly over Facebook, Twitter, or any other social media platform that we use. Sometimes we may invite you to send your details to us via private messaging, for example, to answer a question. You may also be invited to share your personal information through secure channels to participate in other activities, such as competitions.

How do we manage your credit information?

We do not use an individual's personal information to assess their credit eligibility. However, during the course of providing the service to the individual, we may collect credit information that is necessary to provide them with the service.

What kinds of credit information may we collect?

The main kind of credit information we collect is an individual's identification information. However, in the course of providing services to you, we may be given (and subsequently hold) the following other kinds of credit information:

- information about any credit that has been provided to you;
- your repayment history;
- information about your overdue payments;
- if terms and conditions of your credit arrangements are varied;
- if any court proceedings are initiated against you in relation to your credit activities;
- information about any bankruptcy or debt agreements involving you;
- any publicly available information about your credit worthiness; and
- any information about you where you may have fraudulently or otherwise committed a serious credit infringement.

We do not collect your credit information from credit reporting bodies, banks or other credit providers unless it is necessary to provide you with the service or you have expressly asked us to.

How and when do we collect credit information?

In most cases, we will only collect credit information about you if you disclose it to us and it is relevant in providing you with the service.
Other sources we may collect the credit information from include:

- banks and other credit providers;
- other individuals and entities via referrals; and
- your suppliers and creditors.

However, in most cases you will be aware that this information is being collected as part of the service we are providing to you.

How do we store and hold the credit information?

We store and hold credit information in the same manner as outlined earlier in this policy.

Why do we collect the credit information?

Our usual purpose for collecting, holding, using and disclosing credit information about you is to enable us to provide you with the service. We may also collect credit information to process payments.

Overseas disclosure of the credit information

Our outsourced service providers or employees that may be located in the Philippines may have some access to your credit information but generally we will not disclose your credit information to overseas entities unless you expressly advise us to, apart from the following circumstances:

- To the extent that it is necessary or desirable to make such a disclosure to obtain payment of money owed to us.
- Disclosure of information through the use of a cloud or other outsourced information technology services. For example, we may choose to use software providers which store data on overseas servers, such as those previously disclosed in the section under the heading "Do we disclose personal information overseas?".

Your credit information will not be disclosed to overseas recipients unless we are satisfied that the recipient is subject to privacy protection laws that offer substantially similar levels of protection as those required under the APPs or if we have taken reasonable steps to ensure this personal information is handled in a safe and secure manner and that overseas entity is aware of the obligations relating to the information under the APPs.

How can I access my credit information, correct errors or make a complaint?

You can access and correct your credit information, or complain about a breach of your privacy in the same manner as set out in the below section of this policy.

Access to and correction of personal information

It is important that the information we hold about you is up-to-date. You should contact us if your personal information changes.

You can request access to the personal information we hold about you. You can also ask for corrections to be made. To do so, please contact us.

There is no fee for requesting that your personal information is corrected or for us to make corrections. In processing your request for access to your personal information, a reasonable cost may be charged. This charge covers such things as locating the information and supplying it to you and will be disclosed to you prior to being levied

In keeping with our commitment to protect the privacy of personal information, we may not disclose personal information to you without proof of identity.

We may deny access to personal information if:

- the request is unreasonable;
- providing access would have an unreasonable impact on the privacy of another person;
- providing access would pose a serious & imminent threat to the life or health of any person;
- providing access would compromise our professional obligations; or
- there are other legal grounds to deny the request.

If we refuse to give you access to or to correct your personal information we will give you a notice explaining our reasons except where it would be unreasonable to do so*.*

If we refuse your request to correct your personal information, you also have the right to request that a statement be associated with your personal information noting that you disagree with its accuracy*.*

If we refuse your request to access or correct your personal information, we will also provide you with information on how you can complain about the refusal.

If the personal information we hold is not accurate, complete and up-to-date, we will take reasonable steps to correct it so that it is accurate, complete and up-to-date, where it is appropriate to do so.

How do we handle data breaches?

A data breach occurs when personal information is lost or subjected to unauthorised access, use, modification or disclosure or other misuse or interference.
We have implemented a data breach response plan to assist us to effectively contain, evaluate and respond to data breaches in order to mitigate potential harm to any persons affected by a data breach.

In summary, our data breach response plan:

- directs our staff as to the steps they should take in the event of an actual or suspected data breach;
- appoints a team to handle data breaches;
- specifies a strategy for assessing and responding to data breaches;
- sets out the process for notifying any affected persons, the Privacy Commissioner and other relevant parties; and
- outlines the review process to help prevent data breaches in the future.

We will generally notify you if we reasonably believe that your personal information has been subjected to a data breach if:

- there is a risk of serious harm to you;
- notification could enable you to avoid or mitigate serious harm;
- the compromised personal information is sensitive or likely to cause humiliation or embarrassment to you; or
- we are required to notify you by law.

We will notify the Privacy Commissioner if we reasonably believe that your personal information has been subjected to a data breach:

- that is likely to result in serious harm to you; or
- through a third party service provider we have engaged (that stores your personal information overseas) and the data breach is likely to result in serious harm to you.

However, we may not notify you or the Privacy Commissioner if we take action in relation to the data breach before it results in serious harm to you and a reasonable person would conclude that such action was sufficient to ensure that the data breach would not be likely to result in serious harm to you.

Where appropriate, we may also notify other third parties of a data breach.

Resolving your privacy concerns and complaints – your rights

If you wish to complain about an interference with your privacy, then you must follow the following process:

- The complaint must be firstly made to us in writing, using the contact details in this section. We will have a reasonable time to respond to the complaint.
- In the unlikely event the privacy issue cannot be resolved, you may take your complaint to the Office of the Australian Information Commissioner.

We will acknowledge your complaint as soon as we can after receipt of your complaint. We will let you know if we need any further information from you to resolve your complaint.

We aim to resolve complaints as quickly as possible. We strive to resolve complaints within five business days but some complaints take longer to resolve. If your complaint is taking longer, we will let you know what is happening and a date by which you can reasonably expect a response.

Contact us

You can contact us by:

- calling - 07 4160 9000
- emailing - team@bbuscentre.com.au
- visiting - www.bbuscentre.com.au
- writing to us at - PO Box 130, Nanango Qld 4615

Our privacy officer is Tanya Glenny.

Changes to the Privacy Policy

We may change the way we handle personal information from time to time for any reason. If we do so, we will update this Privacy Policy. An up-to-date version is available on www.bbuscentre.com.au or by calling us on 07 4160 9000.
This policy is effective March 2026.

Meaning of words

We, **us** or **our** means:

- Burnett Business Centre Pty Ltd ABN 50 694 157 063
- Burnett Business Centre Financial Planning Pty Ltd ABN 57 117 677 264

and

- Acceber Pty Ltd & Adlemi Pty Ltd trading as Burnett Business Centre ABN 32 015 643 185
- Imelda Mangan and Rebecca Searle ABN 41 272 077 060