(07) 5631 8000 | **bennettandbennett.com.au** | ABN 15 031 964 657 | B.B.H Pty Ltd

Privacy Policy

B.B.H. Pty Ltd ATF BBH Practice Trust trading as Bennett and Bennett Group

(07) 5631 8000 | **bennettandbennett.com.au** | ABN 15 031 964 657 | B.B.H Pty Ltd

Contents

PURPOSE

At Bennett + Bennett, we are committed to protecting the privacy, integrity, and confidentiality of personal information. This Privacy Policy explains how we collect, use, disclose, store, and protect personal information in accordance with the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs), and our ISO 27001 compliant Integrated Management System (IMS).

This policy also aligns with applicable state-based privacy legislation (e.g., Information Privacy Act 2009 (Qld)) where relevant and applies to all personal information, regardless of format or medium (digital, physical, or photographic).

It ensures that all employees, contractors, and third-party users understand their responsibilities for safeguarding personal and company information throughout their engagement with Bennett + Bennett.

This policy applies to all personal information obtained in the course of our operations, including from:

- Current and former employees, contractors, and job applicants
- Clients, suppliers, contractors, and project stakeholders
- Website visitors, service users, and members of the public

We are committed to maintaining trust and transparency in the way we handle personal information.

SCOPE

This policy applies to all personal information collected by Bennett + Bennett through its websites, digital systems, software platforms, training sessions, client interactions, or other business activities. It explains:

- The types of personal information we collect
- How we collect, hold, use, and disclose personal information
- How individuals can access or correct their personal information
- How we protect personal information
- How privacy complaints can be made and managed.

DEFINITIONS

Personal Information: Information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether true or not, and whether recorded in a material form or not (e.g., name, email address, phone number).

Sensitive Information: A subset of personal information that includes information about an individual's health, racial or ethnic origin, political opinions, religious beliefs, sexual orientation, or criminal record, among others. We only collect sensitive information where it is reasonably necessary for our functions (for example, assessing fitness for work or managing workplace injuries) and, where required by law, with your consent.

Data Breach: Unauthorised access to, disclosure of, or loss of personal information.

TYPES OF PERSONAL INFORMATION COLLECTED

The types of personal information we collect may include:

Employees, Contractors & Job Applicants

While managing our systems, fleet and workplaces, we may collect system and activity logs (such as access logs, device identifiers, vehicle telematics, or security footage) for security, safety, compliance, and performance management purposes, in accordance with applicable laws and internal policies.

During recruitment and onboarding, we may collect personal information necessary to assess suitability for employment, including background checks and verification of qualifications. All employment contracts include confidentiality and information security clauses to protect personal and client data.

- Full name, address, and contact details
- Date of birth, employment history, qualifications
- Bank and superannuation details
- Tax File Number (TFN) and government-issued identifiers
- Health or medical information (e.g. fitness for work, workers compensation)
- Emergency contact details

We may also collect accessibility or dietary preferences where relevant to company events or training activities.

Clients, Suppliers, Contractors & Project Stakeholders

- Contact names and details
- Business, property, or project information relevant to our services
- Communication and project history
- Payment and billing details
- Transaction information such as purchase orders or credit account details

This may also include third-party or landowner data supplied by clients or project partners for the purpose of project delivery.

Website Visitors & Online Users

- IP addresses and device identifiers
- Website usage, analytics, and cookies
- Online form submissions and communication records
- Marketing preferences and website interaction data gathered through analytics tools

HOW WE COLLECT INFORMATION

We collect personal information through:

- Direct interactions (contracts, project briefs, onboarding, correspondence)
- Digital platforms, portals, and collaboration tools
- Recruitment agencies, referrals, and third-party partners
- We may also collect personal information from publicly available sources, referees, government databases, or third parties (such as clients or recruitment agencies), where it is unreasonable or impracticable to collect it directly from you.
- On-site activities during service delivery
- Website analytics and cookies

We may also collect information from third-party providers such as analytics services, cloud hosting partners, or client referrals. Information collected automatically via cookies and similar technologies may include browsing activity and preferences.

Where personal information is collected indirectly, we take reasonable steps to ensure individuals are aware of the collection and its purpose.

PURPOSE OF COLLECTION AND USE

We collect, use, and disclose personal information for legitimate business purposes, including to:

- Deliver surveying, spatial, and town planning services
- Manage employment, payroll, and workplace health and safety
- Communicate with clients, suppliers, contractors, and stakeholders
- Process payments and manage accounts
- Conduct business development and marketing (with opt-out options)
- Comply with legal, regulatory, and contractual obligations
- Improve systems, processes, and service delivery

We may also collect and use personal information to deliver or manage software platforms, training services, and customer support.

Personal information may be used for market research or surveys to improve service quality.

DISCLOSURE OF PERSONAL INFORMATION

We may disclose personal information only where required and appropriate, including to:

- Internal business units such as People and Culture, Finance, and Operations
- Government authorities and regulators (e.g. ATO, Fair Work, Safe Work)
- External service providers such as IT, payroll, legal, or accounting consultants
- Insurers, superannuation funds, or employee benefits providers
- Clients, contractors, or project partners, where necessary for service delivery

We may also disclose information to business partners, resellers, or professional advisors who provide support on our behalf, subject to confidentiality and security obligations.

Where legally required, we may disclose information to enforcement or government agencies.

All external disclosures are governed by confidentiality agreements and, where relevant, Data Processing or Supplier Agreements that set out privacy and security expectations.

Cross-Border Disclosure

While we primarily store information in Australia, some service providers (e.g. cloud platforms, collaboration tools) may store or process data overseas. We take reasonable steps to ensure that such disclosures comply with the APPs and are consistent with our ISO 27001 information security controls.

These providers may include Microsoft 365, Abtrac, or other cloud systems hosted in jurisdictions such as the United States or European Union. Bennett + Bennett takes reasonable steps to ensure providers uphold privacy protections equivalent to Australian standards or obtains consent before disclosure.

SECURITY AND STORAGE

We are compliant to ISO 27001 and apply rigorous controls to protect personal information from misuse, loss, unauthorised access, modification, or disclosure. Measures include:

- Secure access controls, authentication, and role-based permissions
- Encryption, firewalls, antivirus protection, and intrusion monitoring
- Secure disposal and destruction of records (physical and electronic)
- Staff training and confidentiality agreements
- Regular audits and risk assessments under our IMS

In addition to technical safeguards, Bennett + Bennett maintains human resource controls to mitigate risks of misuse, loss, or unauthorised access. These include pre-employment screening, confidentiality agreements, role-based permissions, and disciplinary action for non-compliance with security or privacy requirements. All staff are required to complete periodic privacy and security awareness training to maintain vigilance and understanding of their responsibilities.

Information is retained according to our internal retention and disposal schedule, which specifies timeframes aligned with statutory, contractual, and operational requirements. Disposal of information is undertaken via secure destruction or certified digital sanitisation methods. We retain personal information only for as long as necessary to fulfil the purposes outlined in this policy or as required by law or contractual obligations.

Personal information is stored on secure servers managed by reputable hosting providers with multi-layered security, regular patching, and data redundancy protocols.

Privacy and security training is mandatory during onboarding and is refreshed at least annually. The IMS Committee monitors completion rates and reports to leadership as part of management review activities.

DATA BREACH RESPONSE

In the event of a data breach involving personal information, we follow our ISO 27001 incident response procedures and obligations under the *Notifiable Data Breaches (NDB) Scheme*.

- Affected individuals and the Office of the Australian Information Commissioner (OAIC) will be notified where required.
- We will act quickly to contain, assess, and remediate the incident.
- We will promptly assess suspected data breaches. Where an eligible data breach is confirmed, we will notify affected individuals and the OAIC as soon as practicable and in accordance with the Notifiable Data Breaches Scheme. We aim to complete our assessment within 30 days of becoming aware of the incident.

ACCESS AND CORRECTION

Individuals may request access to their personal information or ask for corrections where data is inaccurate, outdated, or incomplete. Requests can be made to our IMS Committee. We will respond within a reasonable timeframe, in line with APP requirements.

Bennett + Bennett may charge a reasonable fee for access where permitted by law, but not for the request itself. If access is refused, written reasons will be provided and the individual may lodge a complaint with the OAIC.

DEALING WITH MINORS

Our services are generally not directed to children. Where we collect personal information about minors, we do so in accordance with applicable laws and, where reasonable, with consent from a parent or guardian.

ANONYMITY AND PSEUDONYMITY

Where practicable, individuals may interact with Bennett + Bennett anonymously or using a pseudonym (e.g., general inquiries). However, identification may be required to provide certain services or meet legal obligations.

COOKIES AND WEBSITE TRACKING

Our websites may use cookies and similar technologies (including third-party analytics providers) to understand website usage and improve our services. Individuals can manage cookie preferences through their browser settings; however, some features may not function properly if cookies are disabled.

MARKETING AND COMMUNICATION

We may use contact details to provide updates about our services, events, or company news. We do not sell personal information. Individuals may opt out of marketing communications at any time by following the unsubscribe link or contacting us directly.

Marketing communications will only be sent in accordance with the Spam Act 2003 (Cth) and will relate to services relevant to our relationship with the recipient.

COMPLAINTS

Privacy-related complaints should be directed to our IMS Committee. We will investigate promptly and respond within a reasonable period. If you are not satisfied, you may contact the Office of the Australian Information Commissioner (OAIC).

Office of the Australian Information Commissioner (OAIC)
Website: www.oaic.gov.au
Phone: 1300 363 992
Email: enquiries@oaic.gov.au

Complaints will be acknowledged within 7 days and resolved within 30 days wherever possible. Outcomes will be communicated in writing, including any corrective actions taken.

POLICY REVIEW

This policy will be reviewed annually or earlier if legislative or operational changes require it. The most current version will always be available on our website.

ROLES AND RESPONSIBILITIES

Parties	Roles and Responsibilities
All Staff & Contractors	Handle personal information in line with this policy, complete privacy and information security training, report breaches or suspicious activity, and comply with confidentiality obligations.
Managers & Team Leaders	Ensure staff understand and comply with privacy and information security expectations; support corrective action where breaches occur.
IT & Systems Administrators	Maintain security of systems, support breach response, and manage disposal.
People & Culture Team	Manage staff data and ensure HR processes (recruitment, onboarding, termination) align with privacy and security requirements, including background checks and confidentiality agreements.
Board of Directors	Ensure policy compliance, promote privacy culture, and review performance under the IMS.
IMS Committee	Acts as the central point of contact for privacy matters, complaints, and compliance monitoring.

MONITORING AND EVALUATION

The IMS Committee is responsible for all monitoring and evaluation of privacy practices across the organisation. The committee will oversee compliance with this policy, ensuring that personal information is collected, stored, and managed in accordance with legal requirements and organisational standards.

This includes:

- Responding to questions regarding privacy practices and this policy
- Reviewing privacy incidents or breaches and ensuring they are appropriately addressed
- Ensuring corrective actions are implemented in line with organisational values and legal obligations
- Maintaining records of privacy-related activities and reporting trends to leadership while protecting individuals' confidentiality

The IMS Committee, which includes a representative of the People & Culture team, ensures employee awareness, onboarding, and disciplinary processes align with information security and privacy expectations.

Any queries regarding this policy or the management of personal information should be directed to the IMS Committee at privacy@bennettandbennett.com.au.

REVISION RECORD

Version	Date	Description
V-01	October 2025	Initial Issue