Privacy Policy & Client Identity Verification Consent

PART 1 – PURPOSE

Colwell Wright Solicitors/Top Gun Conveyancing (ABN 22 095 276 136) are referred to in this Privacy Policy as **we**, **us** or **our**. The purpose of this authority is to ensure compliance with various regulatory frameworks including frameworks which govern your privacy, identity verification and those that allow us to transaction your property electronically (a requirement in Queensland). It also applies to our obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (the AML/CTF Act). It also sets out how we handle your information and for what purposes we will use it. If you have any concerns regarding your privacy or the use of your private information, please let us know.

PART 2 – CLIENT IDENTITY VERIFICATION CONSENT

2.1 Acknowledgment of Legal Requirement

We may be required to verify your identity and collect certain information under the AML/CTF Act when we provide designated services. Identity documents might also be required for other services such as court matters, real property transactions and asset dealings.

This includes collecting identification documents and information about the source of funds and beneficial ownership of entities. You acknowledge that identity verification is mandatory in certain matters, including but not limited to:

- Conveyancing and property transactions
- Electronic lodgement network (including PEXA) transactions
- Trust account matters
- Matters we consider high-value or high-risk transactions

We may be legally prohibited from acting for you if identity verification cannot be completed and reserve the right to terminate our retainer if identity verification standards acceptable to us and required by law cannot be met.

2.2 Express Informed Consent

By signing this document, you expressly consent to:

- Collection of personal information for identity verification;
- Electronic verification through the Digital Verification Service (DVS);
- Verification of identity documents against issuing authority records;
- Use of biometric comparison where lawfully permitted;
- Retention of verification logs and transaction reference numbers;
- Disclosure to authorised government agencies and verification providers strictly for lawful purposes.

Consent is limited to lawful verification and regulatory compliance purposes only.

PART 3 – PRIVACY POLICY

3.1 Types of Personal Information Collected

We collect your contact and identity details, financial information and case related information about you and any relevant entity or person. This may include sensitive information. We may collect:

- Full name, date of birth, residential address

- Government-issued identification documents
- Contact information
- Financial and trust account information
- Transactional information
- Electronic verification metadata
- Audit logs and system access records

Sensitive information is collected only where reasonably necessary and lawful.

3.2 Method of Collection

We collect information directly from our clients, from other lawyers, real estate agents, government sources or public sources such as registers or the internet. Information may be collected:

- Directly from you
- Via electronic verification systems
- From government databases (via Digital Verification Services "DVS")
- From financial institutions
- From property transaction platforms
- From real estate agents
- From authorised third parties, including search providers

We collect only information reasonably necessary for our purpose of providing legal services to you.

3.3 Purpose of Collection

We collect, hold, use and disclose personal information for the primary purpose of providing legal services to our clients, complying with regulatory and insurance obligations and operating our legal practice. Secondary purposes include financial management, system improvement, enforcement of our right to payment and managing the relationship between our firm and former clients once the retainer has concluded. Personal information may be collected for:

1.1. Primary Purposes

This includes:

- providing legal advice and representation to you or to our client(s);
- managing client matters and files;
- conducting legal research and investigations;
- preparing and reviewing legal documents;
- communicating with you and other parties;
- billing and collecting fees, including pursuit of our rights under a Costs Agreement or retainer;
- complying with our legal, professional and insurance obligations; and
- administering and managing our firm.

1.2. Secondary Purposes

We may also use and disclose personal information for secondary purposes that are related to our primary purposes, including:

- maintaining and developing our relationship with you;
- training and professional development;
- ongoing Customer Due Diligence as required by the AML/CTF Act;
- training AI or automated systems including AI development by our vendors with appropriate confidentiality safeguards in place;
- enforcement of our right to payment of fees;

- internal reporting and analysis; and
- risk management and insurance purposes.

We do not use DVS information for unrelated purposes.

3.4 Disclosure of Information

Your personal information and confidential data is held by us subject to our duty of confidentiality under the Australian Solicitor's Conduct Rules ("**ASCR**") and any applicable undertakings or court rules. We may disclose personal information to third parties subject to those obligations and for the purposes described in this Privacy Policy, including:

- to discharge our professional obligations to you or to our clients or in the reasonable execution of our instructions;
- to comply with our legal obligations or in answer to a compulsory notice such as a subpoena or warrant, or to disclose information under the AML/CTF Act, Criminal Code(s), *Legal Profession Act* or other relevant legislation;
- to barristers, mediators, expert witnesses, investigators and consultants and other legal practitioners engaged to act for you (and/or our client) or in relation to the matter;
- other parties to legal proceedings or transactions as instructed, reasonably necessary or required by law;
- courts, tribunals, government agencies and regulators;
- our professional indemnity insurers;
- a Costs Assessor in the event that an assessment is ordered or reasonably necessary.
- service providers who assist us to operate our business (including IT providers, AI providers, document management providers, and marketing service providers);
- related entities;
- as permitted under the ASCR confidentiality exceptions; and
- any person you expressly or impliedly authorise us to disclose information to.

We do not sell or trade personal information.

3.5 Overseas Disclosure

We do not disclose personal information overseas unless required by law or necessary for delivery of our services to you.

3.6 Data Security

We implement reasonable and proportionate safeguards including Encryption, Multi-factor authentication, Role-based access controls, Secure cloud storage, Staff confidentiality obligations and Secure destruction protocols. We hold your personal information using a system designed to protect against data breaches, however like all data security systems, risks may only be mitigated but not eliminated.

3.7 Data Retention

We retain personal information for as long as necessary to fulfil the purposes for which it was collected, to comply with our legal and professional obligations and to ensure that pertinent evidence remains available if reasonably required.

3.8 Access and Correction

You have the right to request access to or correction of the personal information we hold about you. To make an access request, please contact our Privacy Officer (cwreception@colwellwright.com.au).

If we refuse to correct your personal information, we will provide written reasons for the refusal and information about how you may complain.

The Privacy Act permits us to refuse access in some circumstances. If we refuse your access request, we will provide you with written reasons for the refusal (unless unreasonable to do so or we are prohibited from doing so by law) and information about how you may complain.

3.9 Complaints

If you have a question about this policy or complaint about how we have handled your personal information, please contact our Privacy Officer. We ask that you provide details of your complaint in writing. We will acknowledge your complaint within 10 business days and investigate it promptly. We aim to resolve complaints within 30 days. If we need more time, we will keep you informed of our progress.

If you are not satisfied with our response, you may escalate your complaint to:

Office of the Australian Information Commissioner (OAIC) or the Legal Services Commission.

Website: www.oaic.gov.au

Phone: 1300 363 992

Email: enquiries@oaic.gov.au

Post: GPO Box 5218, Sydney NSW 2001

PART 4 – DATA BREACH FRAMEWORK

We maintain a Data Breach Response Plan compliant with the Notifiable Data Breach Scheme. We hold your personal information using a system designed to protect against data breaches, however like all data security systems, risks may only be mitigated but not eliminated. It is our practice to require our storage service providers to be reputable [and to seek assurances from them regarding security and confidentiality]. We retain personal information for as long as necessary to fulfil the purposes for which it was collected, to comply with our legal and professional obligations and to ensure that pertinent evidence remains available if reasonably required. If a data breach is likely to result in serious harm, we will:

- Contain the breach
- Assess risk
- Notify affected individuals
- Notify the Office of the Australian Information Commissioner where required
- Implement remediation measures
