

JV RECRUITMENT
PRIVACY POLICY

Contents

1. Protecting Your Privacy....2
2. Your Implied Consent....2
3. What Information We Collect....2
   3.1. Personal & Candidate Information....2
   3.2. Sensitive Information....3
   3.3. Client, Subcontractor & Commercial Data....3
   3.4. Website & Technical Data....3
4. How We Collect Personal Information....3
5. Artificial Intelligence (AI) and Automated Candidate Screening....4
   5.1. Tools That Support Human Decisions....4
   5.2. Information-Gathering Tools (No Decision-Making)....4
   5.3. AI Training and Candidate Data Protection....4
6. How We Use Your Personal Information....5
7. Sharing and Disclosure of Personal Information....5
8. Overseas Data Disclosures and Hosting Locations....5
9. Data Security and Safeguards....6
10. Data Retention & Destruction....6
11. Notifiable Data Breaches (NDB) Scheme....6
12. Accessing and Correcting Your Information....7
13. Service Communications & Marketing Opt-Out....7
14. Privacy Complaints and Contact Details....7

1. Protecting Your Privacy

JV Recruitment Pty Ltd ABN 27 137 226 852 (referred to in this policy as **"JVR "**, **"we"**, **"us"**, or **"our"**), is committed to protecting your privacy in accordance with the *Privacy Act 1988* (Cth) and the Australian Privacy Principles (APPs).

This Privacy Policy explains how we handle (including collect, store, use, disclose, and safeguard) your personal information across all recruitment, commercial labour hire, site staffing, website, and software platforms operated by the JVR.

2. Your Implied Consent

Whenever you provide personal information to the JVR, regardless of the channel or interaction method used — including through online application forms, online onboarding forms, phone screening calls, in-person screening interviews, digital chat tools, email, or website usage—you consent to our handling of your personal information, as set out in this Privacy Policy.

Your consent permits us to use your personal information to contact you for both core service delivery (such as job matching, shift allocation, and site deployment) and direct marketing purposes (from which you can opt out at any time).

By agreeing to act as your referee, your referee is implied to have given their consent to our handling of their personal information. Please check with your referee and share with them a link to this Privacy Policy. If your referee does not consent to handling of their personal information, please do not provide us with that personal information.

3. What Information We Collect

We collect only that personal and sensitive information that is reasonably necessary to carry out our recruitment, labour hire and workforce management functions.

We aim to avoid collection of personal information about minors and about individuals who are not residents within Australia.

3.1. Personal & Candidate Information

- **Contact & Identity Details:** Full name, residential address, email address, telephone number, birth certificate, passport, permission to work visa, date of birth and emergency contact details.
- **Employment & Qualification Records:** Work history, resumes, qualifications, professional registrations, aptitude assessments, and referee details.
- **Licences & High-Risk Tickets:** Driver's licence details, traffic control accreditations, white card certification, working with children checks, and any associated ticket verification details necessary for site deployment.
- **Placement & Work Records:** Candidate interview recordings, digital signature logs, shift/traffic scheduling records, and reference checks.
- **Financial & Payroll Data:** Bank details, superannuation details, tax file number (TFN), payslips, and payment processing information for placed workers.

3.2. Sensitive Information

- **WorkCover & Injury Management:** Where required for workplace health and safety (WHS), site safety, or WorkCover claims management, we collect medical histories, injury reports, workplace accident details, geolocation tracking data and medical assessment reports for injured workers undergoing rehabilitation or fitness-for-work checks.
- **Criminal Record Checks:** JVR does not collect police checks or criminal record checks as standard recruitment policy.

3.3. Client, Subcontractor & Commercial Data

- **Business Contact Details:** Representative details, market tender extracts, sales prospects, and client credit check data.

3.4. Website & Technical Data

- **Digital Metrics:** Non-personally identifiable browser information, IP addresses, operating systems, page view durations, and referring URLs collected automatically when visiting our website. We do not use digital metrics to collect sensitive personal information.

4. How We Collect Personal Information

We collect personal information directly from you wherever possible, as well as through third-party sources and automated software integrations.

Collection Channel	Source Used
Direct Submissions	Online job application forms, digital onboarding forms, resume uploads, and formal paper/PDF documentation.
Consultant & Dispatch Operations	In-person screening interviews, phone conversations, interactive candidate chat interactions, shift scheduling communications, and interview recordings.
Third Parties	Your details as referee, Reference checks, feedback from former employers or site supervisors, and medical reports from health professionals following WorkCover assessments.
Automated Tools	Website cookies, analytic tools, digital intake tools and automatic candidate resume formatting/parsing tools.

5. Artificial Intelligence (AI) and Automated Candidate Screening

JVR utilises specialised Artificial Intelligence (AI) and automated systems to support recruitment speed and workforce management across our recruitment and traffic operations.

In accordance with statutory automated decision-making disclosure standards, our AI operations are categorised into two distinct operational types:

5.1. Tools That Support Human Decisions

We use automated tools and AI algorithms (including SmartAI and resume parsing software) to assist our personnel in evaluating candidate data.

- **Kinds of Information Used:** Work history, qualifications, tickets, accreditations, geographic locations, resume details, and assessment responses.
- **Kinds of Decisions Involved:** Initial suitability screening, candidate-to-role matching, resume parsing, and shortlisting recommendations for open recruitment or traffic roles.
- **Human Oversight:** These tools do not make automated final determinations. They function strictly as decision-support systems. All final choices regarding candidate shortlisting, client presentation, site allocation, and hiring remain under the direct control and decision-making of our human recruitment consultants and operations personnel.

5.2. Information-Gathering Tools (No Decision-Making)

We deploy automated intake systems, such as website chat tools, automated voice intake tools, and digital application workflows, that collect, format, and provide an administrative process on candidate information.

- **Scope:** These tools solely gather, record, and format details provided directly by candidates. They make no assessment of candidate suitability and play no role in candidate decision-making.

5.3. AI Training and Candidate Data Protection

- **No Training on Identifiable Data:** JVR strictly does not train external or internal AI models on candidates' identifiable personal information.
- **Service Improvement:** De-identified, aggregated data (from which individual identity cannot be derived) may be used to analyse operational trends, enhance system capabilities, and improve service delivery.

6. How We Use Your Personal Information

We handle your personal information primarily to provide recruitment, staffing and workforce solutions. This includes:

- Assessing ongoing work suitability, matching candidate skills to specific roles, and managing site placements.
- Sharing candidate profiles with prospective clients and host employers (strictly with prior candidate consent).
- Processing worker/contractor payments, superannuation, and financial accounting.
- Overseeing workplace safety, injury management, rehabilitation, and compliance under WorkCover regulations.
- Communicating job opportunities, site updates, training sessions, and marketing material via direct mail, email, SMS, or phone (with direct opt-out options provided).

7. Sharing and Disclosure of Personal Information

We do not rent, sell, or trade personal information to third parties for marketing purposes. We disclose personal information only as required to manage our business operations, deliver recruitment services, or comply with legal requirements.

We may disclose your information to:

- **Clients & Host Employers:** Clients seeking permanent staff or temporary labour hire workers.
- **Referees & Accreditation Bodies:** Former employers, licensing authorities, and training organisations to verify tickets and references.
- **WorkCover & Rehabilitation Bodies:** Workers' Compensation authorities, medical practitioners, and insurers involved in workplace injury claims or return-to-work plans.
- **Service Providers & IT Vendors:** External technology providers, hosting facilities, and software platforms supporting our recruitment, financial, and traffic management systems.

8. Overseas Data Disclosures and Hosting Locations

JVR engages specific overseas administrative personnel and uses third-party cloud applications to support its recruitment and traffic operations. Candidate personal information may be accessed or processed in the following designated locations:

Offshore Administrative Support

Philippines: Offshore administrative personnel employed through our vendor partner, assist with backend operations. Access is strictly controlled via Australian-managed environments using secure credentials and multi-factor authentication under Australian IT oversight.

Specific Cloud Software & Storage Locations

Candidate data processed by third-party software platforms utilised by JVR is hosted or processed exclusively within Australia and the following specific overseas jurisdictions:

- **New Zealand**
- **United Kingdom**
- **United States of America**

We do not transfer or disclose candidate data to any overseas locations other than those specified above, and we maintain reasonable safeguards to ensure all overseas providers maintain data security standards comparable to the Australian Privacy Principles.

9. Data Security and Safeguards

JVR employs physical, electronic, and procedural safeguards to protect personal information against loss, unauthorised access, modification, or disclosure:

- **Access Restrictions:** Cloud systems, candidate databases, and shift management platforms are protected by encryption, firewalls, user permission controls, and multi-factor authentication.
- **Local Managed Infrastructure:** Core workspace services are managed locally by our Australian IT service provider.
- **Offshore Security:** Equipment issued by our vendor partner, operates under centralised security policies, ensuring secure connections to JVR's Australian cloud environment.

10. Data Retention & Destruction

We take reasonable steps to securely destroy or permanently de-identify personal information when it is no longer required for any authorised purpose. We may seek your express consent to continue to store your personal information if we have not placed you in a role for more than 12 months.

11. Notifiable Data Breaches (NDB) Scheme

In the event of an unauthorised access, disclosure, or loss of personal information, JVR will conduct an immediate assessment. If the data breach is likely to result in serious harm to individuals and required under the *Privacy Act 1988*, we will notify the Office of the Australian Information Commissioner (OAIC) within 72 hours of becoming aware of the data breach and affected individuals promptly. If not likely to result in serious harm, we will take reasonable steps to prevent or reduce harm to affected individuals.

12. Accessing and Correcting Your Information

You have the right to request access to the personal information we hold about you and to request corrections if it is inaccurate, out-of-date, or incomplete.

- **Submitting a Request:** Requests should be submitted in writing to our Privacy Officer via email.
- **Response Timelines:** We will acknowledge receipt of your request within seven (7) working days and provide a final response or access within 30 working days.
- **Costs & Exceptions:** Requesting access is free, though reasonable administrative costs may apply for retrieving large historical files. If access is withheld under statutory exemptions, we will provide written reasons.
- **Corrections:** We are not obliged to adopt any correction of personal information you provide to us, although we will keep your request with your personal information if that is the case.

13. Service Communications & Marketing Opt-Out

Consent provided across our intake channels includes permission to contact you regarding relevant job placements, operational updates, and marketing communications. You may withdraw consent for marketing communications at any time:

- Click the "Unsubscribe" link at the bottom of any marketing email.
- Reply "STOP" to direct SMS messages.
- Contact us directly at info@jvrecruitment.com.au

14. Privacy Complaints and Contact Details

If you have questions, concerns, or wish to lodge a complaint regarding our handling of your personal information:

Step 1: Internal Complaint

Please submit your complaint in writing to our Privacy Officer:

- **Attention:** Privacy Officer
- **Company:** JV Recruitment Pty Ltd
- **Phone:** 1300 225 558 *(Monday to Friday, Business Hours)*
- **Email:** info@jvrecruitment.com.au
- **Post:** Level 2, 345 Arden Street, Kensington VIC 3031

We will acknowledge your complaint within seven (7) working days and endeavor to investigate and resolve the issue within 30 days.

Step 2: External Review

If you remain dissatisfied with our response, you may escalate your complaint to the independent privacy regulator:

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