PRIVACY POLICY

Infopeople Pty Ltd *(dba Infopeople)* specialises in recruiting ICT, HR, Policy and Procurement personnel across various industries and is a panel supplier for the Australian Government.

We are dedicated to maintaining excellence in the recruitment industry by ensuring our consultants adhere to high standards throughout the recruitment process. This involves thoroughly pre-screening CVs, obtaining references, verifying qualifications and conducting statutory checks before placing any candidate with a client. Our goal is to provide experienced candidates who meet client specifications, comply with legislation and adhere to agreed service levels.

To achieve this, we need to collect personal and at times sensitive information from candidates, contractors and clients. Infopeople is committed to protecting the individuals' privacy and ensuring that the information we hold is used only in ways which the individual has consented.

This Privacy Policy statement is provided to help individuals understand both our processes and how we use the information collected.

Infopeople complies with the National Privacy Principles (Schedule 3 of the Privacy Amendment [Private Sector] Act 2000), a copy of which can be obtained from https://www.oaic.gov.au/.

WHAT INFORMATION DO WE COLLECT?

Infopeople collects the following information:

1. Sufficient information about candidates and contractors to achieve our common objective of payrolling/managing them in the contract positions that align with their skills, experience and job preference.

2. Information that is normally exchanged between an employee and an employer in the context of an employment relationship, including but not limited to tax file numbers, banking details and any information relevant to a worker's compensation claim.

3. The information we typically collect and hold about Clients is necessary for managing the delivery of our services.

4. Aggregated information such as which areas of our website are visited most frequently and which services are used the most. Infopeople reserves the right to share this information with others so that we can continually improve our services. This data will not be linked to any personal information that can identify any individuals.

5. Names, addresses and/or email addresses to enable us to send newsletters. Individuals have the option to "unsubscribe" from these communications at any time.

The information we generally collect to payroll/manage individuals in employment includes:

a) **Personal details** such as name, address, phone numbers and e-mail addresses.
b) **Work history** including employment dates, employer names, duties and achievements.
c) **Education and professional qualifications**.
d) Details of job preferences, remuneration, corporate structures, etc.
e) Client's contact details, job titles, banking details and purchase orders.
f) **Information from referees** to confirm work experience and skills.

We will inform individual prior to conducting reference checks. Infopeople generally does not collect sensitive information such as professional association memberships, health information, or criminal history, unless we have your consent or are required to do so by law.

WHY DO WE COLLECT PERSONAL INFORMATION?

Infopeople collects personal information for the following purposes:

1. To assess skills and qualifications of candidates and determine their suitability for specific roles.

2. To manage our services for clients and communicate effectively throughout the recruitment process.

3. To fulfill client requests for payroll and management of suitable contractors for specific roles, ensuring we have the required personal information to facilitate this payroll process.

WHY DO WE HOLD PERSONAL INFORMATION?

Infopeople holds personal information to:

1. Payroll/manage contractors when they secure positions that align with their skills, experience and job preference.

2. Inform contractors and clients about new job opportunities, services and other relevant information that may benefit them.

3. Comply with statutory obligations to relevant government organisations eg. ATO, etc.

4. Maintain contact with placed contractors to ensure the contract assignment is satisfactory for all parties.

5. Provide ongoing support to placed contractors throughout the duration of their contracts.

HOW DO WE COLLECT PERSONAL INFORMATION?

Most personal information is collected directly from our candidates through the following methods:

1. Telephone calls, email exchanges and interviews.

2. Applications for jobs advertised on our website or a third-party job boards.

3. Information provided by Clients to Infopeople to facilitate payroll and management of contractors' next contract.

Occasionally, we may collect information from third parties, such as referees, etc. In these cases, we will seek each individual's consent for the collection of this information and will take reasonable steps to inform them of:

1. The purpose of collecting the information.

2. Any legal requirements that necessitate the collection of this information.

3. The potential consequences of not providing the information.

HOW DO WE HOLD PERSONAL INFORMATION?

Infopeople holds personal information in a both electronic and paper-based files at our offices and other secure premises. We respect each individual privacy and have implemented measures to ensure that access to this information is restricted to Infopeople staff who require it for their roles.

HOW IS PERSONAL INFORMATION USED AND DISCLOSED?

Personal information is used for the purposes for which it was collected and held, as outlined above. By providing us with personal information, individuals consent to its collection and internal use in accordance with this Privacy Policy.

However, individuals will be contacted to provide consent prior to their personal information is disclosed to a third party, They will be advised of the particular purpose of the disclosure. Consent is usually sought in writing or via email. The only exception is when disclosure is required by law or by an enforcement agency.

CAN AN INDIVIDUAL ACCESS PERSONAL INFORMATION HELD BY INFOPEOPLE?

Yes, any individual can:

1. Request a copy of their personal information.
2. Request corrections or updates to their personal information
3. Request removal of their personal information from our files.

Note: The above does not apply to information held on employees of Infopeople.

Process for Requesting Access:

1. Provide proof of identity.

2. Make the request in writing.

3. Infopeople will provide the information within 30 days, usually within a few days.

4. A fee will be charged and payable to Infopeople to cover the cost of identifying and copying information held. The fee will be charged at the rate of $50.00 per hour with the minimum being $25.00. We will provide an estimate of the cost at the time of the request.

HOW CAN A COMPLAINT BE MADE?

1. For complaints about how we handle personal information, candidates or contractors should contact our Contracts Manager. We will respond to the complaint as quickly as possible but not later than 28 days after receiving it.

2. If dissatisfied with our response or outcome of the enquiry, the complaint can be escalated to the Office of the Federal Privacy Commissioner. The office is located at Level 8, Piccadilly Tower, 133 Castlereagh Street, Sydney, NSW, 2000. Their telephone number 1300 363 992.

HOW DO WE DELETE/DESTROY PERSONAL INFORMATION?

1. We follow a data retention policy with defined retention periods.

2. Physical records are destroyed through methods such as shredding or incineration, while electronic data is securely deleted using techniques like data wiping and degaussing.

3. We document the destruction process and conduct regular audits to ensure compliance.

4. We provide training to employees on these procedures, ensure third-party compliance and regularly review and update our policies to adhere to legal and regulatory standards.

HOW DO WE PROTECT PERSONAL INFORMATION?

1. **Physical Security Controls:** Restricted access to facilities, surveillance systems and technical measures such as data encryption (in transit and at rest), firewalls, intrusion detection systems (IDS) and multi-factor authentication (MFA).

2. **Access Controls:** Ensuring that only authorized personnel can access sensitive data and regular software updates protect against vulnerabilities.

3. **Regular Security Audits and Risk Assessments**: Conducting audits and assessment to identify and mitigate risks, providing ongoing employee training on data protection practices and enforcing strict policies and procedures for data handling.

4. **Incident Response Plan**: An established plan to quickly address and manage any security breaches.

HOW DO WE PROTECT AGAINST PERSONAL INFORMATION MISUSE?

1. We maintain comprehensive audit logs that track access and modifications to personal data, and regularly review these logs for suspicious activities.

2. Role-based access and multi-factor authentication are enforced to ensure that only authorised personnel can access sensitive information.

3. User access is reviewed periodically, and security audits are conducted to ensure compliance with our policies.

4. We provide ongoing training for employees on security awareness and have strict policies and procedures in place to manage and respond to potential misuse or unauthorised access effectively.

HOW DO WE DETECT AND RECTIFY PERSONAL INFORMATION MISUSE?

1. We continuously monitor our systems for unusual activity that could indicate a breach and train staff on recognise signs of potential breaches and report them promptly.

2. We quickly assess the scope and nature of the suspected breach to determine its potential impact, gathering relevant data and logs to understand what occurred and the extent of the breach.

3. Immediate steps are taken to contain the breach, preventing further unauthorised access of data loss. We also identify and implement measures to rectify vulnerabilities that led to the breach.

4. We have a plan in place for notifying clients about the breach, including details on what information was compromised and steps being taken. This plan ensures compliance with legal obligations regarding breach notification to authorities and affected individuals.