

PRIVACY POLICY

Macweld Crane Hire is committed to complying with privacy obligations and taking all reasonable steps to ensure that personal and sensitive information is managed appropriately.

It is the obligation and responsibility of every employee to ensure that privacy and personal information is protected in accordance with this policy. The General Manager Strategy, Risk & Projects (Fleurieu Cranes) is the Privacy Officer and is responsible for ensuring our compliance with the Australian Privacy Principles (APPs) and the Privacy Act 1988 (Cth) (the Privacy Act) where applicable and to receive and respond to all complaints and queries. All employees are required to comply with the APPs and the Privacy Act.

This policy sets out how we manage personal information.

Employee records as defined in the Privacy Act means a record of personal information relating to the employment of an employee. This includes health information about an employee and personal information about all or any of the following:

- the engagement, training, disciplining or resignation of an employee;
- the termination of the employment of an employee;
- the terms and conditions of employment of an employee;
- an employee's personal and emergency contact details;
- an employee's performance or conduct;
- an employee's hours of employment;
- an employee's salary or wages;
- an employee's membership of a professional or trade association;
- an employee's trade union membership;
- an employee's recreation, long service, sick, personal, maternity, paternity or other leave;
- an employee's taxation, banking or superannuation affairs

Personal Information as defined in the Privacy Act as information or an opinion about an identified individual (or in which the individual is reasonably identifiable) regardless of whether it is true or not, and whether it is recorded in a material form or not. Examples of personal information include names, addresses, email addresses, phone numbers and dates of birth.

Sensitive information as defined in the Privacy Act means:

- information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, or criminal record that is also personal information; or
- health information about an individual; or
- genetic information about an individual that is not otherwise health information; or
- biometric information that is to be used for the purpose of automated biometric verification; or
- biometric templates.

We collect and maintain personal information about our clients, visitors and guests, employees, volunteers, subcontractors, consultants and suppliers. This policy covers the collection, use and dealings with this information. It does not apply to records excluded by the Privacy Act.

What Information Do We Collect?

We only collect and hold information that is directly relevant to and reasonably necessary for the management of business activities in order to provide a comprehensive service. We may collect and maintain records that may contain personal information about our clients, visitors and guests, employees, volunteers, subcontractors, consultants, suppliers and partners.

Depending on how a person interacts with us, we may collect, use and hold various types of personal information about the person, which includes but is not limited to:

- contact and personal details (including name, date of birth, gender, qualifications, phone number, email address, and home and office address),
- credit card details, bank account details and payment and purchase/transaction history,
- records of their communications and other interactions with us, including via email, phone, via our company website, from publicly available sources, from cookies and from third parties,
- business partners' and sub-contractors' personal information, including business contact information, business experience, financial details, contract details, services or goods provided or offered, induction records, qualifications, referees, other credit and finance related information, and information provided as a part of the assessment process,
- criminal records or medical records to the extent that it is relevant to our functions and responsibilities, and
- the technology used to access our services.

We will ensure that the personal information it collects, uses and discloses is accurate, up to date, complete and relevant to its management of employees and business activities.

We may have to collect and use sensitive information about a person for the purpose of performing our functions and activities. Sensitive information can be collected across a variety of circumstances. For example, during site inductions, or where a person is ill, injured or involved in some incident on our premises and we need to collect your medical information to allow us to properly investigate, process and/or report the incident to our insurer and the relevant authorities. It can also arise where there are suspicions of unlawful activity or serious misconduct, or the information is necessary for the health and safety of an individual or the public or to meet client compliance and mandatory reporting obligations. Sensitive information will only ever be collected when it is lawful and authorised under Australian law, and/or a person provides us with consent to the collection of the information.

Why do we collect, use and disclose personal information?

We will only use or disclose personal information for the primary purpose for which we have collected that information.

The purposes for which we collect, hold, use and disclose personal information includes:

to conduct our business, which includes providing our services;

- to comply with any law, regulation, rule or requirement of any government authority; including but not limited to work health and safety laws, and record-keeping requirements under the Fair Work Act 2009 (Cth);
- for security, safety, operational and risk management purposes (e.g. security monitoring, emergency and incidents monitoring, investigation and reporting);
- for internal administrative, record-keeping, research, planning, marketing and product or service development purposes;
- to provide effective personal (employee, sub-contractor, consultant, visitor etc.) care;
- to process and respond to any enquiry or complaint made by the person;
- to consider a job application; and
- to consider a contract with business partners and sub-contractors.

We will not hold, use or disclose personal information for any secondary purpose, unless the person consents and/or it is permitted under Australian law. Personal information can also be used where the secondary purposes closely related to the primary purpose in circumstances where it would be reasonably expected that such use or disclosure would occur.

Where reasonable and practicable to do so, we will collect personal and sensitive information only from the person whose information it is. However, in some circumstances we may be provided with information by third

parties, for example when conducting police checks or medical assessments or where we have received the information through recruitment agencies.

How do we collect the information?

We collect personal information about people in the provision of our services and management of its business. We collect information directly from a person in a variety of ways depending on each business relationship (including verbally and in writing) whether it is over the phone, in person, by accessing and using our website, posting about us on social media, attending company premises, entering into a contract with us or applying for a job.

In some situations, we may also indirectly collect personal information from third parties, including business partners, credit reporting agencies, recruitment agencies, law enforcement agencies, other government authorities or entities, and previous employers or referees for job applicants.

Where we have not taken active steps to collect personal information and receive unsolicited personal information, we will destroy or de-identify the information, where appropriate, as promptly as practicable. For example, upon receipt of any misdirected documents in electronic or hardcopy form, a reply will be promptly made to the sender advising of the error and the document will be deleted or destroyed.

Disclosure of Information

We will only disclose personal information to other individuals or organisations for the primary purpose for which the information was collected, with consent or as permitted by law, or for a secondary purpose as outlined above.

We may disclose personal information to those parties that are involved in providing, managing or administering our services. This could include:

- organisations involved in our business activities including our business partners, sub-contractors, suppliers, clients, agents, and debt collectors;
- organisations involved in our payment systems including banks and payment organisations;
- organisations that maintain, review and develop our business systems, procedures and technology infrastructure including IT service providers;
- professional advisors such as accountants, insurers, lawyers and auditors; and
- body corporates that are associated with us.

The collection, handling and usage of employee records are exempt from the Privacy Act and this policy. We, however, will observe strict confidentiality, and ensure the proper and secure management of our employee records.

Many of our customers require employee information for security checks and other compliance related reasons. We will seek consent from employees to provide information to customers and suppliers for our employees attending their sites. The types of information requested included driver's licences, tickets and other qualifications which may or may not include personal information.

Macweld Crane Hire is unlikely to disclose personal information to overseas recipients.

We may use personal information for the purpose of sending direct marketing communications unless a person advises us that they do not want this to occur. A person can withdraw their consent to any direct marketing at any time by following the opt-out or unsubscribe instructions, or contacting us.

Security & Access

Personal and sensitive information is stored in a manner that reasonably protects it from misuse and loss and from unauthorised access, modification or disclosure. We have taken reasonable steps to ensure the integrity and security of the personal information we hold, including restricted server access, encryption, standard security protocol, firewalls and complex password protection. Such steps protect the personal information that we hold from misuse, interference and loss, and from unauthorised access, modification or disclosure.

When personal or sensitive information is no longer needed for the purpose for which it was obtained, we will take reasonable steps to destroy or permanently de-identify personal information. However, most of the personal information is or will be stored in files which will be kept by us for a minimum of 7 years.

The owner of the information that we hold may access all of their personal information. They can correct the personal information if it is inaccurate, out of date, incomplete, irrelevant or misleading.

All requests to access or correct personal information should be in writing and submitted to the Privacy Officer. We will respond to the request within a reasonable period of time after we have received the request. We will not charge any fee for any access request but may charge an administrative fee for providing a copy of personal information to the authorised entity.

To protect personal and sensitive information we may require identification from parties wishing to access the information before releasing the requested information.

We may refuse to approve a request to access or correction if there is a reason under the Privacy Act or any other law. If we do refuse access or correction, we will provide the inquirer with written notice, and include the reasons for refusing.

Quality

It is important to us that personal information is up to date. We will take reasonable steps to make sure that personal information is accurate, complete and up to date. If you find that the information we have is not up to date or is inaccurate, please advise us as soon as practicable via the method outlined above.

Complaints

If a person believes there has been a breach of the APPs, or a registered APP code that binds us, and they wish to make a complaint about how we have handled their personal information, they can submit a complaint in writing to the Privacy Officer.

We will respond to the complaint within 30 days or within such other time frame as is reasonable in the circumstances. If a person does not consider our response to their complaint satisfactory or the complaint is not resolved, the complaint can be referred to the Office of the Australian Information Commissioner at www.oaic.gov.au.

Contact Us

If there are any queries about this policy, you may direct your query to the Privacy Officer using the contact details set out below.

Privacy Officer

Cesar Federici

cesar.federici@fleurieucranes.com.au

08 8260 5122

Postal address:

7-9 Lafitte Road, WINGFIELD SA 5013

Brandon Freer



10 April 2024

MANAGING DIRECTOR

SIGNATURE

DATE