1. Privacy Policy

We are committed to protecting the privacy of personal information. We will take all reasonable steps to ensure that the collection, use, disclosure and handling of all personal information complies with the Privacy Act 1988 (Cth) ["the Act"] and the Australian Privacy Principles ["APP's"].

A copy of this policy can be obtained by visiting the Employer's website or contacting our Privacy Officer (insert Privacy Officer name).

2. Scope

This policy applies to all customers, suppliers, patients and their families, employees, visitors, contractors, consultants and other representatives engaged by the Employer and to those who have a legitimate business need to access personal information in the course of performing their duties.

3. Responsibility

The obligations imposed on the Employer under this policy are also imposed on any individual employed or engaged by the Employer. If a representative of our Group discloses personal information, that individual must take steps as are reasonable in the circumstances to ensure that the third party does not breach the APPs in relation to the information.

All matters concerning information privacy (IP) are to be directed initially to the Manager, or where necessary to our Privacy Officer:

Mrs Kristine Griggs
Griggs Haulage Contractors
(07) 4782 9350
ghc@griggshaulage.com.au

4. Definitions

Personal Information is defined as information or an opinion about an identified individual, or an individual who is identifiable: whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not.

Health information is any information about a person's health or disability, and any information that relates to a health service they have received, are receiving or will receive. Health information is sensitive and personal, which is why there are laws to protect the rights of individuals in keeping their information private.

Sensitive information is a type of personal information such as: race or ethnic origin, political opinions, religious or philosophical beliefs, sexual preferences and orientation, health information and criminal record. If mishandled, this information may result in discrimination or harm.

5. Collection of Personal Information

Typical examples of personal information collected by the Employer include:

- Names, address, email address and telephone numbers.
- Financial information such as credit card number and banking information.
- Employment related information including employment records, training, performance and conduct information, taxation, banking, superannuation details and professional associations.
- Employee, contractor and consultant personal information including addresses, contact numbers, gender, age, employment history, references, resume, medical history, criminal record, emergency contacts, qualifications and licenses.
- Resumes, contact details, references and qualifications for the purpose of assessing suitability for employment.
- General correspondence and/or notes detailing conversations.

Personal information will be collected directly from the individual whose information it is. However, there may be circumstances (e.g. due to health) where we may need to collect information from, or talk to someone else, for example the individual's medical representatives, attorney, carer or a relative.

6. Data Protection

We use a variety of security measures to help prevent unauthorised access to improper use of personally identifiable information.

Our employees and other representatives are required to take steps as are reasonable in the circumstances to protect personal information from misuse, interference, loss and from unauthorised access, modification or disclosure.

Our security measures include:

- Training our employees in privacy matters (i.e., via this Handbook).
- Limiting or restricting access to information to those with a legitimate business need.
- Physical security of documents in locked rooms and filing cabinets.
- Appropriate building security and access controls.
- Password protection on all electronic and wireless devices.
- Regular and continuous monitoring of our IT systems.
- Installation and maintenance of firewalls to prevent hacker attacks.
- Installation and maintenance of anti-malware programs on computers and servers.
- Restriction and secure storage of laptops/notepads to those employees who need them.
- Obtaining consent for the use of photographs that identify any individual.

If we hold personal information that we are not required by law to retain the information, we will take such steps as are reasonable in the circumstances to destroy the information or to ensure it is de-identified within the timeframes stipulated by any relevant authorities or retention schedules.

Where we have reasonable grounds to believe that an eligible data breach (as defined in legislation) has occurred, or in instances where it is directed to do so by the Commissioner, it will provide relevant notification to the Office of the Australian Information Commissioner (OAIC) and/or to affected individuals.

7. Policy Review

This policy will next be reviewed on 29 February 2026.