TABLE OF CONTENTS

1.0 PURPOSE

Hardings Group wants everyone who interacts with the business to feel confident that their personal information is respected and protected.

This Privacy Policy sets out how personal information is collected, used, stored, and shared, and outlines the rights individuals have under the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs).

2.0 SCOPE

This policy applies to all employees, contractors, job applicants, clients, external parties and other individuals who provide personal information to Hardings Group.

3.0 RESPONSIBILITIES

Executive Management	• Make sure the policy is in place and followed. • Undertake investigations and appropriate action if a privacy breach takes place. • Review serious privacy breaches or complaints and reporting them to the board where needed. • Report to the Government in the event of a notifiable breach.

HR	• Ensure all employees and external parties are made aware of this policy and understand their responsibilities. • Ensure this policy is accessible to external parties covered by the policy • Keep all related records secure and confidential. • Support investigations if a privacy breach takes place.
Project Managers/ Coordinators/ Team Leaders	• Handle personal and confidential information respectfully. • Store employee and client information securely and only allow access where appropriate. • Direct team members to HR if they have privacy-related questions or need to update their details.
Employees *These responsibilities apply to everyone at Hardings Group, including Project Managers, Team Leaders, and Executive Management.*	• Only collect or access personal information if it's part of your role or necessary to complete a job. • Keep information private and follow the right steps for storing or disposing of it. • Report any privacy concerns or suspected breaches to your manager or HR straight away.
External Parties *Clients, Contractors, Consultants, Third-Party providers such as RTO's*	• Use information only for the agreed project, service, or contractual purpose. • Protect confidential information by storing it securely. • Share or disclose information only with authorised people who need it. • Comply with the Privacy Act 1988 (Cth), the Australian Privacy Principles, and contractual confidentiality obligations. • Notify Hardings Group immediately of any suspected or actual privacy breach. • Return or securely destroy Hardings Group's information at the end of the engagement unless retention is legally required.

4.0 DEFINITIONS

Personal information	Any information that can identify someone, such as their name, contact details, ID documents, or health records, whether it's written down or not.
Sensitive Information	This includes racial background, religious beliefs, union membership, criminal history, or health information. These details are protected under privacy law and must be handled with care.
Health Information	Personal information about someone's physical or mental health, including medical history, test results, or anything collected to support their wellbeing at work.
Privacy Breach	When someone's personal information is lost, shared, or accessed without permission.
Data Security	The tools and processes we use to keep personal information safe, such as like locked filing cabinets, password protection, two factor authentication (2FA), secure servers, and access controls that limit who can see what.

The definitions are based on the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs).

5.0 TYPES OF PERSONAL INFORMATION COLLECTED

Hardings Group only collects personal information that is needed to run its day-to-day operations or meet legal obligations.

This may include:

- **Personal Details:** Name, date of birth, job title, and ID documents such as a driver's licence or passport.
- **Contact Details:** Residential address, phone numbers, email, and emergency contacts.
- **Sensitive Information:** With consent or when legally required: health details, criminal history, union membership, or background checks.
- **Employment-Related Information:** Resumes, licences, qualifications, references, and training records.
- **Images and Footage:** ID photos, CCTV recordings, or project-related images.
- **Government Identifiers:** Such as a tax file number (TFN), Unique Student Identifier (USI).
- **Financial Information:** Bank account details, Superannuation details, credit card information, credit history.

You are not required to share anything you are uncomfortable with, especially sensitive information.

That choice will be respected.

However, if certain details are essential for safety, legal compliance, or access (such as for employment or site entry), not providing them might affect Hardings Group's ability to employ you, provide services, or allow you access to certain sites or systems.

6.0 METHODS OF COLLECTING PERSONAL INFORMATION

Hardings Group collects personal information through several channels.

The main ways personal information is collected include:

Direct Contact

- When someone contacts Hardings Group via the website, email, phone, or in person, details such as name, contact information, and the nature of the enquiry are collected to allow appropriate follow-up.

Job Applications

- When applying for a job or contract role, applicant's information such as a resume, work history, licences, and references is collected to support recruitment decisions.

Induction and Training

- Employees and contractors complete their inductions and training through Lucidity, a secure third-party system. Personal details entered into this system are managed in line with this policy.

Social Media and Subscriptions

- Basic information such as a username or email address may be collected when someone follows the business on social media, subscribes to updates, or sends a message.

Site Visits and Phone Calls

- Personal details may be recorded during site visits, guest sign-ins, inductions, or phone conversations with employees.

Third-Party Sources

- Information may also be received from others, such as referees, labour hire agencies, or clients providing names for site access. This information is treated with the same level of care as if provided directly.

Website Tools

- Cookies and analytics tools may collect non-identifying data (such as browser type, pages viewed) to help improve website performance. Browser settings can be adjusted to block cookies if preferred.

All personal information is collected lawfully. If unsolicited information is received, it will be reviewed, and securely deleted or de-identified if not required, in line with privacy laws.

7.0 REASONS FOR COLLECTING PERSONAL INFORMATION

Hardings Group collects and uses personal information to run its operations and deliver services effectively. Information is only used in ways that are necessary, legally required, or reasonably expected in the course of business.

The main ways personal information is used include:

Delivering Services

- Details may be used to prepare quotes, plan and deliver projects, communicate with clients, manage job progress, send updates, and handle invoicing and payments.

Responding to Enquiries

- When someone contacts Hardings Group with a question or request, their information is used to provide the right support. Occasional updates about services or terms may be shared, and marketing messages are only sent if permission has been given. Opt-out is always available.

Recruitment and People Management

- For job applicants, employees, or contractors, personal information helps manage recruitment, onboarding, training, payroll, and workplace safety. Medical information may be used if needed for insurance or emergency needs.

Safety and Legal Obligations

- Information may be collected to meet safety requirements, such as verifying licences, granting site access, or preparing for emergencies. Medical conditions may also be recorded to support a safe work environment.

Operations and Compliance

- Certain details are used to support day-to-day operations. It includes recordkeeping, audits, responding to complaints, and meeting tax or employment law requirements. Information may be shared with regulators if required by law.

Review

- Feedback, complaints, and incident reports may be reviewed to help improve service quality, processes, or systems. Wherever possible, information is de-identified before it is used for internal reporting.

Financial Management

- To process payroll, reimbursements, superannuation contributions, invoicing, and client payments. Bank account details, superannuation information, and on occasion credit card details are used only for legitimate financial transactions and are handled with strict security measures.

Hardings Group does not use personal information for unrelated purposes unless legally allowed or consent has been provided.

8.0 SHARING PERSONAL INFORMATION

Hardings Group only shares personal information when it is necessary.

When that is the case, only relevant details are provided, and steps are taken to ensure the information is handled securely.

The main circumstances where personal information may be shared include:

Service Providers, Contractors, Training Providers and Medical Professionals

- Information may be shared with trusted providers such as IT support, payroll platforms, HR systems, legal advisers, consultants, accountants, training organisations, or medical practitioners/ ITPs, strictly for delivering their services.
- These providers are required to meet data protection standards.

Clients and Project Partners

- In the course of delivering a project, basic information (such as names or induction status) may be shared with contractors, site managers, or other project stakeholders.

Legal or Emergency Situations

- Details may be disclosed to regulators, law enforcement, or emergency services when legally required or where there is a serious risk to health or safety.

With Consent

- If personal information is ever used outside of everyday business needs (for example publishing a testimonial, or using images for social media), written consent will be sought first.

Hardings Group does not sell personal information and does not share it for third-party marketing.

All information shared is done so with a legitimate business or safety purpose.

9.0 STORAGE OF PERSONAL INFORMATION

Information is stored in both physical and digital formats, and practical steps are taken to keep it secure and accessible only to those who need it.

The main ways personal information is kept secure include:

Paper Records

- Hard copy documents are only maintained for employee records, such as signed forms or employment records. These physical records are stored in locked cabinets, with access limited to HR and payroll.

Digital Security

- Electronic records are protected by secure servers, password-protected systems, antivirus software, and role-based access controls. This means team members only see the information that is relevant to their role. IT Managed Service provides continuous 24/7 monitoring for potential security breaches, enhancing protection and rapid response to any threats.

Third-Party Systems

- Some information is stored through trusted platforms and software (such as payroll, induction systems, or email providers). These providers are carefully selected and meet Australian Privacy and Data Security standards.

Ongoing Safeguards

- Internal systems and procedures are reviewed regularly to keep data protection practices up to date. Once information is no longer needed, it is securely deleted or destroyed or de-identified.

Hardings Group acknowledges that no system is immune to risk but takes all reasonable precautions to keep your information safe and minimise security threats.

10.0 DISPOSAL OF PERSONAL INFORMATION

Hardings Group only keeps personal information for as long as it is needed, for business, legal, or compliance reasons. Once it is no longer required, it is securely destroyed or de-identified.

The retention period depends on the type of record. For example, employee and financial records may need to be kept for up to 7 years, sometimes longer.

Safety records, incident reports, and other compliance-related files may also be retained for insurance or legal reasons.

Records are reviewed regularly, and anything no longer required is removed.

The main ways personal information is kept and disposed of include:

Secure Disposal Methods

- When it is time to dispose of information, Hardings Group takes appropriate steps to protect privacy. Paper records are securely shredded or destroyed.
- Digital files are permanently deleted or wiped from systems.
- Where data needs to be kept for reporting or planning, it may be de-identified so that no individuals can be identified.

Archived Records

- Some records may be archived in case they are needed in the future, for example, for legal or insurance purposes.
- Archived information is stored securely, with limited access, and is removed or anonymised once it is no longer needed.

These practices help make sure that personal information is managed responsibly and not kept longer than necessary.

For specific details about how long certain types of information are retained, Hardings Group can provide further guidance.

11.0 ACCESSING PERSONAL INFORMATION

11.1 Internal requests

Individuals have the right to request access to their personal information held by Hardings Group.

The steps below explain how to access it:

1. **Make a Request**
    - Access requests must be made in writing, either by email or letter (see Contact Details at the end of this document).
    - Clear details about the type of information being requested will help speed up the process.
    - Proof of identity will be required to ensure the request is valid.

2. **Timeframe for response**
    - Hardings Group aims to respond within 30 days.
    - If the request cannot be fully met, a written explanation will be provided.

3. **Delivery Format**
    - Where possible, information will be shared in the preferred format, such as email, print, or in-person review.
    - For complex requests, the information may be provided in stages.

11.2 When access may be limited or refused

Access may be declined in limited circumstances, such as when:

- It would compromise someone else's privacy or safety
- It is linked to ongoing legal matters or court orders
- It breaches a law or regulation
- It relates to an active investigation

If access is refused, a written explanation will be provided along with guidance on next steps or how to make a complaint.

11.3 Third party requests

Personal information will not be released to others without written consent or legal authority (for example power of attorney).

If a third party, such as a lawyer or insurer, submits a request, documentation confirming the individual's authorisation will be required.

12.0 UPDATING PERSONAL INFORMATION

If personal information is incorrect, incomplete, or out of date, a request can be made to have it corrected.

How to request a correction

- Send a written request, by email or letter, with the details that need updating and what the correct information should be. For more significant updates, supporting documents may be requested (for example, if there is a dispute about accuracy).

How long it takes

- Hardings Group aims to respond within 30 days. Simple updates may be made sooner. If the incorrect details were shared with other parties, they may also be notified of the correction if necessary.

What happens if a change cannot be made

- If the update is declined, a written explanation will be provided. A request can also be made to add a note to the file to reflect the individual's view.

13.0 RAISING A PRIVACY CONCERN OR COMPLAINT

Questions or concerns about how personal information is handled are always taken seriously.

How to make a complaint

- Concerns can be raised by contacting Hardings Group using the contact details listed below. It is helpful to include as much information as possible, what happened, when, and how privacy may have been affected. Complaints are best submitted in writing (by email or letter) to ensure a clear record and support a thorough review.

What happens next

- Complaints will be acknowledged within a few business days. If more information is needed, this will be requested. Most matters are resolved within 30 days, and regular updates will be provided throughout the process. If a privacy breach is confirmed, Hardings Group will explain what happened and how it will be addressed.

If the outcome is not satisfactory

- If the matter is not resolved or the outcome is not satisfactory, a complaint can be lodged with the Office of the Australian Information Commissioner (OAIC) at www.oaic.gov.au.

14.0 CONTACT

For questions about this policy, or to request access, make a correction, or raise a privacy concern, please contact:

Hardings Group

30 Industrial Drive

Ulverstone, TAS 7315

Phone: (03) 6425 7557

Email: admin@hardingsgroup.com.au

POLICY AUTHORISATION

This policy has been reviewed and authorised by Hardings Group (TAS) Pty Ltd. It reflects the standards, expectations, and responsibilities applicable to all relevant personnel.

Should any changes be made to this policy, Hardings Group (TAS) Pty Ltd will communicate those changes through the established communication methods within the company.

This policy is effective from the date of authorisation and remains in effect until it is formally amended or withdrawn by Hardings Group (TAS) Pty Ltd.

Authorising Name:	Nic Broomhall
Authorising Position:	Chief Executive Officer (CEO)
Authorising Signature:	
Authorising Date:	12/03/2026