ERES GROUP

SOLAR MAINTENANCE SPECIALISTS

UK | AUS

Privacy & Data Handling Policy

Internal policy on the handling, security and retention of information

Document title	Privacy & Data Handling Policy
Document reference	EG-AU-POL-002
Version	1.0
Issue date	8 September 2026
Next review date	8 September 2027
Document owner	Managing Director, Eres Group
Approved by	Scott Simmons, Managing Director

This document is the property of Eres Group Pty Ltd. It is reviewed at least annually, or sooner where changes in legislation, guidance or business activities require it. Printed copies are uncontrolled — the latest version is held by the Document Owner.

1. Purpose

This policy sets out how everyone at Eres Group in Australia must handle personal information and confidential business information. It exists to ensure information is handled lawfully and securely in line with the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs), and that the commitments in our public Privacy Policy (EG-AU-POL-001) are delivered in practice.

2. Scope

This policy applies to all directors, employees, engineers, temporary workers, subcontractors and anyone else handling information on behalf of Eres Group in Australia. It covers personal information about clients, site and property contacts, suppliers, subcontractors and staff; all formats — electronic records, emails, business systems, photographs and thermal imagery, and paper records such as job sheets, quotes and compliance certificates; and all locations — our premises, client sites, vehicles, home working and mobile devices. It also covers confidential company information — pricing, financial records, banking details and commercial terms — which must be protected with the same care.

3. Key definitions

Personal information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable — e.g. a name, contact details, or a property address linked to an occupier.
Sensitive information	A special category including health information, requiring extra protection and generally consent to collect.
APPs	The 13 Australian Privacy Principles in the Privacy Act 1988 (Cth), covering collection, use, disclosure, quality, security, access and correction.
Eligible data breach	Unauthorised access to, disclosure of, or loss of personal information likely to result in serious harm to an individual — triggering the Notifiable Data Breaches scheme.
Privacy Officer	The person responsible for privacy compliance day to day: [Scott Simmons], contactable via info@eresgroup.com.au.

4. Core principles

Everyone handling information for Eres Group must ensure personal information is: collected only when needed for our work, by lawful and fair means; used and disclosed only for the purposes it was collected for (or as the person would reasonably expect, or as the law allows); accurate, complete and up to date; protected from misuse, interference, loss and unauthorised access; and destroyed or de-identified when no longer needed. The company must also be able to demonstrate compliance through its records, contracts, training and this policy.

5. Responsibilities

Role	Responsibilities
Managing Director	Overall accountability for privacy and data handling; approves this policy and ensures adequate resources.

Role	Responsibilities
Privacy Officer ([Scott Simmons])	Day-to-day oversight: advises staff, handles access, correction and complaint requests, manages breach assessment and notification, and keeps this policy under review.
Managers and supervisors	Ensure their teams understand and follow this policy; ensure new starters receive privacy induction; escalate concerns promptly.
All staff and engineers	Follow this policy and the practical rules below; complete training; report any breach, loss or concern immediately.
Subcontractors and suppliers	Handle information only as instructed, under terms consistent with this policy and the APPs.

6. Day-to-day data handling rules

- Only collect and use the information you need for the job in hand — no more.
- Only access information you need for your role. Do not browse records out of curiosity.
- Keep client, site and account information confidential. Do not discuss it with anyone who does not need to know, and never post it on social media.
- Send personal or confidential information only to verified recipients — double-check email addresses before sending, and use secure sharing methods for anything sensitive.
- Company bank details, payroll information, tax file numbers and similar confidential records must only be handled by authorised staff and never shared externally without the Managing Director's approval. Tax file numbers are subject to specific legal restrictions and must be stored securely and used only for their lawful purpose.
- Keep paper records (job sheets, quotes, certificates) secure — do not leave them visible in vehicles or on client sites, and return them for filing or secure disposal.
- Take photographs and thermal imagery only as needed to record the condition of equipment and property. Avoid capturing people; if a person is inadvertently captured, delete or crop the image where practicable.
- Do not store company data in personal email accounts or personal cloud storage.

7. Devices, systems and security

- Access to business systems is controlled by individual accounts with strong passwords; accounts must not be shared, and multi-factor authentication is used where available.
- Company laptops, tablets and phones must be protected by a passcode or biometric lock, kept updated, and encrypted where supported.
- Devices and paper records must never be left unattended in vehicles overnight and must be stored securely when not in use.
- Software updates and anti-malware protection must be applied promptly; unapproved software must not be installed on company devices.
- Access rights are removed promptly when someone leaves the company or changes role.
- Data is backed up regularly, and backups are tested so records can be restored after loss or failure.

- Confidential paper waste must be shredded or placed in secure destruction bins, never in general waste or recycling.

8. Access, correction and complaints

Any request from an individual to access or correct their personal information, or any privacy complaint — however it is phrased and whoever receives it — must be passed to the Privacy Officer on the same working day. The Privacy Officer will log the request, verify identity where necessary, and respond within 30 days. Staff must never delete or alter records because a request or complaint has been received.

9. Data breaches

A data breach includes lost or stolen devices or paperwork, emails sent to the wrong recipient, unauthorised access to systems, and accidental deletion or disclosure. If you know or suspect a breach:

- Report it immediately — and in any event within 24 hours — to the Privacy Officer. Reporting quickly will never be treated as a disciplinary matter in itself; concealing a breach will.
- The Privacy Officer will contain and assess the breach. Where it may be an eligible data breach, the assessment will be completed promptly and within 30 days at the latest.
- If the breach is likely to result in serious harm to any individual, the OAIC and affected individuals will be notified as required by the Notifiable Data Breaches scheme.
- Every breach is recorded in the breach register, and causes are reviewed so controls can be improved.

10. Sharing information and engaging suppliers

Personal information may only be disclosed outside Eres Group for the purposes in our Privacy Policy. Before engaging any new supplier or system that will handle personal information, staff must obtain approval from the Privacy Officer, who will ensure appropriate due diligence and contract terms. Disclosures to our UK operations or other overseas recipients must comply with APP 8 — reasonable steps to ensure the recipient handles the information consistently with the APPs.

11. Retention and disposal

Record type	Retention period
Enquiries and quotations not leading to a contract	Up to 2 years
Contracts, invoices and financial/tax records	At least 5 years (taxation law)
Employee records (including pay, leave, hours)	7 years (Fair Work Act requirements)
Installation, servicing, certification and warranty records	Life of the installed system or warranty period, whichever is longer
Work health and safety records (incidents, notifiable incidents)	Statutory minimum periods; at least 5 years from incident
Site images incidentally containing individuals	Deleted or de-identified as soon as practicable

When a retention period expires, electronic data must be securely deleted and paper records shredded or placed in secure destruction.

12. Training, compliance and review

All new starters receive privacy guidance as part of induction, with refreshers at least annually or when this policy materially changes. Compliance is a condition of employment and of engagement for subcontractors; failures may be dealt with under our disciplinary procedures or contract terms, and serious breaches can expose the company to regulatory action by the OAIC. The Managing Director owns this policy; the Privacy Officer reviews it at least annually.