FRONTLINE

PROJECTS AUSTRALIA

Privacy Policy

Revision History

Version	Title	Name	Date
V1.0	Initial	RK	27052024
V2.0	Revised branding and compliance review	JK	12112026

Contents

Title	Page Number
Purpose	1
Scope	1
Our Commitment	1
Personal Information We Collect	2
Sensitive Information	2
How We Collect Personal Information	3
Why We Collect, Use and Disclose Personal Information	3
Who We Disclose Personal Information To	4
Overseas Disclosure	4
Automated Decision-Making	5
Storage, Security and Retention	5
Data Breaches	5
Direct Marketing	6
Accessing and Correcting Your Information	6
Complaints	6
Contact Us	6
Review of this Policy	7

Purpose

Frontline Projects Australia Pty Ltd (ABN 72 666 018 113) (**Frontline**, **we**, **us**, **our**) respects your privacy. This Privacy Policy explains how we collect, hold, use, disclose and protect personal information, and how you can access or correct your information or make a complaint.

This policy is prepared in accordance with the Privacy Act 1988 (Cth) (**Privacy Act**), including the Australian Privacy Principles (**APPs**). It is available free of charge on our website at **www.frontlineprojectsaustralia.com.au** and in hard copy on request.

Scope

This policy applies to all personal information handled by Frontline, including information about job applicants, employees, subcontractors and their workers, consultants, suppliers, clients, site visitors, and members of the community near our sites. It applies to all Frontline employees and contractors, who must comply with it.

Government Contracts

Where we handle personal information under a contract with the Commonwealth (including Department of Defence Estate Works Program projects), we are a contracted service provider and comply with the APPs and any privacy obligations in that contract. Where we handle personal information under a contract with a Queensland Government agency (for example, Department of Education school projects), we comply with the Queensland Privacy Principles under the Information Privacy Act 2009 (Qld) where the contract requires it, as well as any contractual privacy clauses. Where a contract imposes stricter requirements than this policy, the contract prevails.

Employee Records

Under the Privacy Act, records relating to the employment of our current and former employees are generally exempt from the APPs when handled for the employment relationship. Frontline nevertheless protects employee records in line with this policy as a matter of good practice. Tax file numbers are handled in accordance with the Privacy (Tax File Number) Rule 2015.

Our Commitment

As a veteran-owned contractor delivering Commonwealth and State Government projects, Frontline takes the security of personal and government information seriously. We aim not only to comply with the Privacy Act, but to apply Commonwealth security standards as far as reasonably practicable for the size, scale and capability of our organisation.

Handling of security-classified or official Commonwealth information (which may not be personal information) is governed separately by our Cyber Security Policy (POAI1.28) and our obligations under the Defence Industry Security Program and relevant contracts.

Our employees and contractors receive privacy training at induction and when this policy changes,

and training is recorded in our training register.

Personal Information We Collect

Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable. We only collect personal information that is reasonably necessary for our functions and activities. The kinds of information we collect depend on how you deal with us:

Who	Kinds of personal information
Job applicants	Name, contact details, resume, employment history, qualifications, licences, referee comments, right-to-work information, and veteran service history where you choose to provide it.
Employees	As above, plus date of birth, emergency contacts, tax file number, bank and superannuation details, payroll and leave records, QLeave registration details, performance and training records, and security clearance details.
Subcontractors, consultants and their workers	Names and contact details, ABN, licences, tickets and competencies (e.g. White Card, high-risk work licences), insurance details, induction and training records, site attendance records, and QLeave details where relevant.
Clients, suppliers and business contacts	Names, job titles, contact details and correspondence.
Site visitors and community members	Names, contact details, site sign-in records, enquiries or complaints.
Website users	Information submitted through our website contact form.

Sensitive Information

Sensitive information includes health information, criminal records and certain other categories, and receives extra protection under the Privacy Act. We only collect sensitive information where it is reasonably necessary for our functions **and** you consent, or where the law otherwise permits or requires it. The sensitive information we may collect includes:

- ✓ health and fitness-for-work information, injury, incident and workers' compensation records;
- ✓ information you choose to share under our Mental Health and Suicide Prevention Policy (POAI1-34), which is handled confidentially and only shared with your consent or where required to protect health and safety;
- ✓ criminal history information required for security clearances, Defence site access, or Working with Children (Blue Card) checks for school sites; and
- ✓ information about veteran status or service history, where you choose to provide it.

How We Collect Personal Information

Where practicable, we collect personal information directly from you, for example through employment applications, onboarding forms, site inductions, prequalification documents, emails, phone calls and meetings. We may also collect personal information from third parties, including:

- ✓ recruitment platforms and agencies (e.g. SEEK, LinkedIn) and referees;
- ✓ your employer, where you work for one of our subcontractors;
- ✓ our clients, including Commonwealth and Queensland Government agencies, for project and site-access purposes;
- ✓ background check providers and government bodies (e.g. AGSVA, Blue Card Services, licensing authorities); and
- ✓ our site management systems (e.g. HammerTech, Procore).

Collection Notices

When we collect personal information, we will take reasonable steps to tell you who we are, why we are collecting it, who we usually disclose it to, and how to access this policy. We do this through collection notices on our key forms, including employment applications, onboarding and induction forms, subcontractor prequalification, and our website contact form.

Unsolicited Information

If we receive personal information we did not ask for and could not have lawfully collected, we will destroy or de-identify it as soon as practicable, where it is lawful and reasonable to do so.

Anonymity

You may deal with us anonymously or using a pseudonym where it is lawful and practicable, such as for general enquiries or community feedback. This is not practicable for employment, engagement as a subcontractor, or access to our sites.

Why We Collect, Use and Disclose Personal Information

We collect, use and disclose personal information for the following purposes:

- ✓ recruiting, employing and managing our workforce, including payroll, superannuation, leave and QLeave obligations;
- ✓ engaging, prequalifying and managing subcontractors, consultants and suppliers;
- ✓ managing work health and safety, site inductions, site access, incident reporting and return-to-work;
- ✓ delivering projects and meeting reporting obligations to our clients, including Commonwealth and Queensland Government agencies;
- ✓ meeting security vetting and site-access requirements for Defence and school sites;
- ✓ tendering, including providing staff resumes and qualifications to prospective clients;

- ✓ managing insurance, claims and legal matters;
- ✓ responding to enquiries and complaints; and
- ✓ complying with our legal obligations.

We will only use or disclose personal information for another (secondary) purpose where:

a) you have consented;

b) you would reasonably expect us to use it for that purpose and the purpose is related to the original purpose (or, for sensitive information, directly related);

c) it is required or authorised by an Australian law or a court or tribunal order;

d) a permitted general situation exists, such as lessening or preventing a serious threat to life, health or safety, taking action on suspected unlawful activity or serious misconduct, or establishing or defending a legal claim; or

e) it is reasonably necessary for enforcement-related activities conducted by, or on behalf of, an enforcement body.

Who We Disclose Personal Information To

Depending on the purpose, we may disclose personal information to:

- ✓ our clients, including Commonwealth and Queensland Government agencies, and their representatives;
- ✓ principal contractors, subcontractors and consultants working on the same project;
- ✓ regulators and government bodies, such as WHSQ, Comcare, QBCC, QLeave, the ATO and the OAIC;
- ✓ security vetting and screening bodies (e.g. AGSVA, Blue Card Services);
- ✓ our insurers, insurance brokers, lawyers, accountants and auditors (including ISO certification bodies);
- ✓ superannuation funds, payroll and banking providers; and
- ✓ IT, cloud and software service providers who store or process information on our behalf.

We do not sell personal information.

Overseas Disclosure

We use cloud-based systems to store and manage information, including (e.g. Microsoft 365 / SharePoint, HammerTech, Procore, Xero).

Before disclosing personal information overseas, we take reasonable steps to ensure the recipient handles it consistently with the APPs. Information held under Commonwealth or Queensland Government contracts is stored in accordance with any data-location requirements of those contracts.

Automated Decision-Making

Frontline does not use computer programs to make, or substantially assist in making, decisions that could significantly affect an individual's rights or interests.

Storage, Security and Retention

We hold personal information in electronic systems and, where necessary, in secure paper files. We take reasonable steps, including technical and organisational measures, to protect personal information from misuse, interference, loss, and unauthorised access, modification or disclosure. These include:

- ✓ multi-factor authentication and role-based access controls on our systems;
- ✓ restricting access to personal information to staff who need it for their role;
- ✓ our Cyber Security Policy (POAI1.28)
- ✓ secure storage and disposal of paper records; and
- ✓ privacy and cyber security training for staff.

We keep personal information only for as long as it is needed for the purpose it was collected or as required by law (for example, employment, tax, WHS and contract records). When information is no longer needed, we take reasonable steps to destroy or de-identify it.

We take reasonable steps to ensure the personal information we hold is accurate, up to date and complete. Please tell us if your details change.

Data Breaches

If we suspect a data breach, we will act quickly to contain it and complete an assessment within 30 days. If a breach is likely to result in serious harm to any individual, we will notify affected individuals and the Office of the Australian Information Commissioner (**OAIC**) as required by the Notifiable Data Breaches scheme. We will also notify any client whose contract requires notification, within the timeframe that contract specifies. Breaches are managed under our Data Breach Response Plan (POAI1.36).

Direct Marketing

Frontline does not use personal information for direct marketing.

Accessing and Correcting Your Information

You may request access to, or correction of, the personal information we hold about you by contacting Managing Director (see Contact Us). We will verify your identity before acting on your request.

We will respond within 30 days. We do not charge for making a request, but may charge a reasonable fee for providing access where large volumes of information are involved. If we refuse access or correction, we will tell you why in writing and how you can complain. If we refuse to correct your information, you may ask us to attach a statement to it noting that you believe it is inaccurate.

Complaints

If you believe we have breached the APPs or mishandled your personal information, please contact our Managing Director in writing (see Contact Us). We will:

a) acknowledge your complaint within 7 days;

b) investigate and keep you informed of progress; and

c) provide a written response within 30 days.

If you are not satisfied with our response, you may complain to the OAIC:

- ✓ Website: www.oaic.gov.au
- ✓ Phone: 1300 363 992

Contact Us

For questions about this policy, or to make a request or complaint, please contact:

Contact	Details
Role	Managing Director
Email	regan@fpaust.com.au
Phone	0420 441 676
Post	Frontline Projects Australia Pty Ltd, 255 Grassdale Road, Gumdale QLD 4154

Review of this Policy

This policy will be reviewed at least annually, and whenever there are changes to privacy law, our systems, or our contractual obligations. The current version will always be available on our website. This version takes effect on 12 November 2026 and has been approved by the Managing Director.

FRONTLINE

PROJECTS AUSTRALIA

VETERAN OWNED BUSINESS CERTIFIED