

## General Privacy Policy

Policy Owner	Director IT
Effective Date	19 Sept 2025
Last Revised	19 Sept 2025
Replaces	Privacy Policy
Approved By	
Review Cycle	Annual

### Introduction

Disaster Relief Australia (DRA) is committed to protecting the privacy and security of personal information. We collect, store, and use personal information in accordance with the **Australian Privacy Principles (APPs) outlined in the Privacy Act 1988 (Cth)**. This policy explains how we handle personal information provided to us by volunteers, members of the public, and other stakeholders.

By accessing our services or providing personal information, you agree to the terms outlined in this Privacy Policy.

### What Information We Collect

We collect personal and sensitive information in various circumstances, including:

- **Volunteers:** We collect personal details, demographic information, medical records, employment history, qualifications, national police checks and defence force service history.
- **Employees:** All staff are volunteers, as such all the information we collect on volunteers are also collected for staff. We also collect payment details for staff members.
- **Members of the Public:** During disaster operations, we may collect personal information such as names, contact details, address, and details regarding the individual's circumstances and needs via platforms such as FulcrumApp.
- **Other Individuals:** Occasionally, we may collect information from other individuals interacting with us, such as councils, other volunteer organisations, contractors or partners.

## How We Collect Personal Information

We collect personal information in several ways, including:

- Through our online application forms and portals (such as Power Pages linked to Dynamics 365, ELMO).
- Via online surveys (Microsoft Forms) for training or operational purposes.
- Through mobile data collection platforms like FulcrumApp during disaster operations.
- By phone, email, paper forms or face-to-face interactions when engaging with our services.

## Use of Personal Information

The personal information we collect is used for the following purposes:

- Assessing volunteer employment applications and qualifications for operational deployments.
- Communicating with volunteers and employees, for the purposes of training, and coordinating deployments.
- Responding to and managing disaster recovery operations, including assessing the needs of individuals affected by disasters.
- Analysing and improving our services to better respond to disaster situations.

We only collect the personal information necessary for these purposes and ensure that sensitive data is handled responsibly.

People may interact anonymously or under a pseudonym where lawful and practicable however, should the person wish to volunteer with DRA, they must provide their legal name.

## Disclosure of Information

DRA does not share personal information externally unless required by law or where specific consent is obtained. We may share anonymised, aggregated data to provide operational reports to our stakeholders or partners.

In cases where personal information needs to be shared with government agencies (e.g., during disaster operations), we ensure all data is either anonymised or personal identifiers are removed, as far as possible. Only designated personnel within the IT department have the authority to manage and approve such disclosures.

## Disclosure to Service Providers

Disaster Relief Australia may engage third-party service providers—including IT support, system administrators, data storage vendors, and digital tools providers (e.g., FulcrumApp)—to support its operations. These providers may have access to personal information of our volunteers or disaster recovery recipients only to the extent necessary to deliver their services.

All service providers are contractually bound to adhere to strict privacy and confidentiality obligations aligned with the Australian Privacy Principles under the Privacy Act 1988 (Cth). Access to personal information is limited, controlled, and monitored, and where providers are located overseas, we take reasonable steps to ensure their compliance with Australian privacy requirements. For example, Fulcrum is owned and managed in the US however, all data is kept within Australian servers.

## Data Security

We take cybersecurity seriously and have implemented measures to protect personal information, including:

- **Encryption:** All personal data stored within Dynamics 365 and other platforms is encrypted at rest.
- **Access Controls:** Access to personal and sensitive information is restricted based on security roles and reviewed regularly to ensure compliance.
- **Cybersecurity Standards:** DRA has achieved Maturity Level 2 in the Australian Government's Essential 8 cybersecurity framework and employs tools such as CrowdStrike for proactive monitoring and incident response.

Additionally, we conduct regular penetration testing and audits to ensure our security measures remain effective.

## Data Retention and Destruction

We retain personal information for the period necessary to fulfil the purposes outlined in this policy:

- **Active Volunteers:** Information is kept while volunteers are active and involved in operations.

- **Inactive Volunteers:** Personal information is retained for 1 year after the volunteer becomes inactive.
- **Public Information (FulcrumApp):** Data collected during operations is kept for 6 months and then securely deleted.

Data that is no longer required is securely destroyed in accordance with our data retention policy.

## Marketing

DRA uses marketing for recruitment and donation purposes. Where someone has been contacted via email or text, there must be an option to unsubscribe from the marketing channel.

## Access to Personal Information

Individuals have the right to access their personal information held by DRA. If you would like to request access or make corrections to your data, please contact us via:

- **Email:** [privacy@disasterreliefaus.org](mailto:privacy@disasterreliefaus.org)

We will verify your identity before providing access to any personal information and aim to respond to requests within 30 days.

## Complaints

If you have any concerns or complaints about how we handle your personal information, please contact us using the details below. We take privacy seriously and will promptly address any issues in accordance with the **Privacy Act 1988 (Cth)**.

## Definitions

- **Personal Identifiable Information (PII):** This includes any information that can identify an individual, especially when combined with other data points. Examples include:
  - Full name (when stored with other information such as contact details, date of birth, or employment history).
  - Date of birth
  - Contact details (e.g., phone number, email address, residential address)
  - Identification numbers (e.g., driver's licence, passport number)

- **Sensitive Information:** This is a special category of PII that requires higher protection due to its nature, such as:
  - Medical or health information
  - Defence force service history
  - Racial or ethnic origin
  - Criminal records or security clearance status

### Context:

A name on its own may not be considered PII under the APPs, as it does not uniquely identify an individual. However, when a name is stored together with other identifying information (e.g., address, date of birth, medical history), it constitutes PII and must be treated with the appropriate level of security.

## Contact Information

For privacy-related questions or concerns, please contact our Privacy Officer at:

**Email:** [privacy@disasterreliefaus.org](mailto:privacy@disasterreliefaus.org)

**Phone:** 1300 372 287

**Mail:** G1, 10 Greenhill Road, Wayville, 5034