



## PRIVACY POLICY

Last updated: 24 February 2026

Compliant with Privacy Act 1988 (Cth), Australian Privacy Principles, and Online Safety Regulations

### INTRODUCTION

Ready Take Action (“RTA”, “we”, “us”, “our”) (ABN: 33 248 239 140) owns and administers the Ready Take Action platform, which may be operated by external third parties under a licence arrangement. We are committed to protecting your personal information in accordance with the Privacy Act 1988 (Cth) (“Privacy Act”) and the Australian Privacy Principles (APPs).

This Privacy Policy explains how we collect, use, disclose, store, and protect your personal information when you use the Ready Take Action website, mobile app, and any related services (collectively, “Platform”).

Third-party operators and promoters, including licence-holders, of the Platform may have their own Privacy Policy.

#### 1. TYPES OF INFORMATION WE COLLECT

We collect information directly from you, automatically through device interactions, and via approved third-party data sources.

##### 1.1 Personal Information (APPs 3 & 5)

This includes information that identifies or reasonably identifies you:

- Full name, date of birth, gender (optional)
- Email address, phone numbers, residential address
- GPS location data (with explicit consent)
- Household information: family members, pets, dependants, special needs
- Property details: property type, risk factors, preparation status
- Emergency planning data: contacts, evacuation plans, checklists
- Health & sensitive information (voluntarily provided): mobility needs, medical conditions, medications
- Insurance information: policy numbers, claims documentation
- Payment information for subscriptions (processed via third-party payment providers)

- Business information for business accounts: ABN, continuity planning data
- Photos, videos, hazard reports, incident reports, and user-generated content

## 1.2 Sensitive Information

We may collect sensitive information (as defined in the Privacy Act), including health data, only with your consent and only where necessary for emergency preparedness, safeguarding, or Platform functionality.

## 1.3 Usage, Technical & Analytical Data

We collect:

- Device information: IP address, operating system, browser, device type
- App interactions: features used, training progress, preparedness scores
- Emergency interactions: SOS activations, alerts viewed/dismissed
- Communication logs: email delivery, notification preferences
- Offline and cached data stored on your device
- Custom events to support analytics, performance and service improvement
- Cookies and tracking data for functionality, analytics, and security

## 1.4 Third-Party Information Sources

- Government emergency feeds (e.g., BOM, SES, CFA, RFS, QFES)
- Weather and location-based risk information
- AI-generated content from third-party LLM providers (queries anonymised where possible)
- Data supplied by insurers or emergency agencies during active emergencies
- Age or identity information from third-party verification services (where required)

## 2. HOW WE COLLECT PERSONAL INFORMATION

We collect personal information through:

- Account registration and user input
- Device permission grants (GPS, notifications, photo uploads)
- Interaction with the Platform (app or website)
- Emails, forms, surveys, and customer support requests
- Social login (Google, Microsoft, Facebook)
- Uploaded documentation (insurance, identity verification, hazard photos)
- Emergency activations (SOS)
- Third-party organisations providing permitted data feeds

### 2.1 Collection from Third Parties

We may also collect information from:

- Emergency agencies
- Identity verification partners
- AI service providers (aggregated/anonymous)
- Payment processors

- Cloud and hosting providers

Where required, we take reasonable steps to notify you of such collection.

## 2.2 Unsolicited Information

If we receive unsolicited personal information, we will promptly destroy or de-identify it unless required for legal or operational reasons.

## 3. HOW WE USE YOUR INFORMATION (APP 6)

We use your personal information for the following purposes:

### 3.1 Primary Purpose – Emergency Preparedness & Response

- Delivering location-based alerts
- Generating personalised safety plans & risk assessments
- Enabling SOS features to assist emergency responders
- Providing real-time hazard information

### 3.2 Platform Operations & Service Delivery

- Managing accounts, authentication & subscriptions
- Synchronising data across multiple devices
- Offline access to critical information
- Enabling community features (volunteer coordination, hazard reporting)

### 3.3 AI-Powered Personalisation

- Producing customised action plans and checklists
- AI-generated insights (data anonymised where technically possible)

### 3.4 Communications

- Emergency notifications (cannot be disabled)
- Service updates, feature announcements
- Optional newsletters and marketing communications (opt-in only)

### 3.5 Research, Analytics & User Experience Improvement

- App usage analysis
- Performance monitoring
- System optimisation
- Disaster preparedness research (de-identified)

### 3.6 Legal, Safety & Fraud Prevention

- Compliance with Australian law
- Responding to lawful requests from authorities
- Detecting misuse or fraudulent activity
- Protecting platform integrity and user safety

We will never use your data for purposes beyond those outlined unless you provide explicit consent.

#### 4. STORAGE & SECURITY OF PERSONAL INFORMATION (APP 11)

We take reasonable steps to protect your information.

##### 4.1 Security Measures

- SSL/TLS encryption for data in transit
- Encryption applied to sensitive data at rest
- Password & credential security
- Firewalls, access controls & audit logging
- Secure token-based authentication
- Regular penetration testing and vulnerability assessments
- Data minimisation and restricted access for staff
- Encrypted local storage (IndexedDB) for offline use

##### 4.2 Social Login Security

If you log in via Google/Microsoft/Facebook, we rely on their MFA/security systems.

##### 4.3 Data Breaches

We comply with the Notifiable Data Breaches Scheme.

If a breach is likely to cause serious harm, we will notify you and the OAIC.

#### 5. MULTI-FACTOR AUTHENTICATION (MFA)

While RTA does not yet support built-in MFA for email/password users, we strongly recommend enabling MFA through social login providers and secure email accounts.

#### 6. DATA STORAGE LOCATIONS (APP 8 – CROSS-BORDER DISCLOSURE)

Your data may be stored or processed in:

- Australia (primary storage)
- United States
- Singapore

We ensure overseas providers:

- Are bound by contractual privacy protections, and
- Use industry-standard security controls.

#### 7. DATA SHARING WITH THIRD PARTIES

We may disclose information to:

- Emergency services during SOS or critical incidents
- Cloud and hosting providers
- Payment processors
- Email and communication platforms
- Analytics providers (aggregated)
- Insurers or emergency agencies for safety purposes

- Government authorities where required by law
- Volunteers and community coordinators (limited and consent-based)

#### 7.1 No Sale of Personal Information

We never sell, rent, or trade your personal information.

#### 8. LOCATION DATA & GPS (APP 3 – EXPLICIT CONSENT)

GPS data is used only when required and only with your explicit consent.

You may disable location sharing at any time, but emergency features may be limited.

Location information is collected when:

- You manually set your home or watch locations
- You enable GPS permissions
- You activate travel mode
- You activate SOS features

Retention: Location history is stored for 90 days, then deleted.

#### 9. AGE VERIFICATION & CHILDREN'S PRIVACY

- Minimum age: 13
- Ages 13–15 require parental/guardian consent
- Ages 16+ required for community/social features
- Under-13 household information may only be entered by parents/guardians

#### 10. IDENTITY VERIFICATION

We may require verification for:

- Age-restricted features
- Insurance-related documentation
- Access to sensitive information
- Fraud risk mitigation
- Account recovery

Documents are encrypted and deleted within 90 days unless legally required.

#### 11. CONSENT & WITHDRAWAL OF CONSENT

We obtain consent for:

- Location services
- Push notifications
- Marketing communications
- Uploading photos/media
- AI-powered plan generation
- Community profile visibility

Emergency alerts cannot be fully disabled for public-safety reasons.

You may withdraw consent at any time; however, some Platform features may become unavailable.

## 12. DATA RETENTION (APP 11)

We retain information only as long as necessary for:

- Emergency preparedness services
- Legal or regulatory requirements
- Risk management and historical analysis

Account deletion: Data is permanently deleted within 90 days (except where legally retained).

Inactive accounts: Deleted after 3 years unless essential data remains relevant.

## 13. AUTOMATED DECISION-MAKING & AI

- Automated suggestions do not replace human judgment
- Humans remain responsible for safety decisions
- No critical emergency decisions are made solely by AI
- You may opt out of AI-generated recommendations

## 14. COOKIES & TRACKING TECHNOLOGIES

We use:

- Essential cookies
- Analytics cookies
- Local storage for offline functionality
- No advertising trackers or third-party marketing cookies

You may adjust browser settings to limit cookies.

## 15. ACCESS, CORRECTION & YOUR PRIVACY RIGHTS (APPs 12 & 13)

You have the right to:

- Request access to your personal information
- Request correction of inaccurate or outdated data
- Request deletion of your account
- Export your data (JSON/CSV)
- Opt out of marketing communications
- Lodge a complaint with the OAIC

Requests may be submitted to: [connect@readytakeaction.com](mailto:connect@readytakeaction.com)

## 16. PRIVACY COMPLAINTS

Step 1 — Contact Us

Email: [connect@readytakeaction.com](mailto:connect@readytakeaction.com)

Phone: 1300 170 880

We will respond within 30 days.

## Step 2 — OAIC

Website: [www.oaic.gov.au](http://www.oaic.gov.au)

Phone: 1300 363 992

Email: [enquiries@oaic.gov.au](mailto:enquiries@oaic.gov.au)

### 17. CHANGES TO THIS POLICY

We may update this policy to reflect:

- Changes to law
- Platform improvements
- New features
- Updated emergency-management requirements

Material changes will be communicated through email and in-app notifications.

### 18. CONTACT DETAILS

Ready Take Action

PO Box 220, Strathdale VIC 3550

Email: [connect@readytakeaction.com](mailto:connect@readytakeaction.com)

Attn: Privacy Officer