Headfirst

Simpler Software/Headfirst Security, Privacy & Compliance

Simpler Software Pty. Ltd., Contact hello@simpler.software
(Version 1.1. Last updated: 27 March 2026)

1. Data Storage & Location

All Headfirst data is stored exclusively on Amazon Web Services (AWS) infrastructure in Sydney, Australia. Data is not stored, processed, or transferred outside of Australia.

Backup replicas are stored in a secondary AWS region in Melbourne, Australia for disaster recovery purposes.

2. Encryption

- **At rest:** All data is encrypted using AES-256 encryption, including the database, file storage, and all backups.
- **In transit:** All connections are secured using TLS 1.2 or higher. HTTP requests are automatically redirected to HTTPS. SSL certificates are managed by AWS Certificate Manager and renewed automatically.

3. Backups & Disaster Recovery

Headfirst maintains three tiers of automated database backups:

- Daily for 30 days
- Weekly for 12 weeks
- Monthly for 1 year

All backups are encrypted and replicated to a geographically separate AWS region (Melbourne) for disaster recovery. Backup completion is actively monitored and alerts are triggered if any backup fails.

Additionally, the database is configured for Multi-AZ (multiple availability zone) deployment, providing automatic failover to a standby replica in the event of infrastructure failure.

4. Access Control

Headfirst uses role-based access control to ensure users only see data relevant to their role:

- **Club Admin**: Full access to all teams, players, reports, and club settings within their club.
- **Trainer / First Aider**: Access only to the teams and players they have been assigned to by the club admin.

Key access control principles:

- A user can only create an account if invited by a club admin.
- No user can access data from another club.
- Club admins control all user access: inviting, assigning teams, deactivating, and deleting users.
- Deactivating a user immediately blocks their access to the app and all club data.
- Users are scoped to their club at login. Switching between clubs (for users with multiple roles) is explicitly controlled.

5. Authentication

- User passwords are hashed using industry-standard one-way hashing and are never stored in plain text.
- The mobile app uses token-based authentication with automatic session expiry.
- Password reset requires email verification.

6. Application Security

Security is integrated into our development process:

- **Automated vulnerability scanning** runs on every code change before deployment, including static analysis for application security vulnerabilities and dependency checking against known CVE databases.
- **Content Security Policy** headers protect against cross-site scripting (XSS) attacks.
- **CSRF protection** is enabled on all form submissions.
- **Code review** is required before changes are merged.
- All infrastructure is defined as code, version-controlled, and deployed through automated pipelines.

7. Privacy & Compliance

Headfirst is designed with privacy in mind, particularly given we handle junior player information.

- **Minimal data collection:** We collect only the data necessary for injury reporting and team management: player name, team, and age group. We do not collect dates of birth, home addresses, or parent/guardian personal information.
- **Injury reports** contain incident details (injury type, treatment provided, venue) recorded by the trainer at the time of the incident. No medical history or sensitive health identifiers are collected.
- **Australian data residency:** All data is stored on AWS servers in Australia and is not transferred overseas.
- **Australian privacy law:** While Headfirst operates as a small business and is not required to comply with the Australian Privacy Principles (APPs), we voluntarily follow APP guidelines as best practice. We encourage clubs to review our approach against their own privacy obligations.
- **Child safety considerations:**
    - The platform collects only publicly accessible information about minors (name, team, age group).
    - Only club-invited and club-approved users can access the platform.
    - Trainers see only the players and teams they are assigned to.
    - There is no public-facing profile, searchable directory, or social features.
    - All user accounts require email verification and password authentication.

8. Data Ownership & Portability

The club owns all data entered into Headfirst. At any time, clubs can:

- **Export** injury reports to CSV format via the portal or mobile app.
- **Request** a full data export by contacting support.
- ` by notifying us via email. We will export all club data to CSV and subsequently delete it from our servers.

Data is retained for the duration of the subscription. Upon contract exit, data is exported and deleted within 30 days of the exit request.

9. System Reliability

Headfirst runs on AWS infrastructure designed for high availability:

- **Application:** Redundant instances run simultaneously with automatic failover. Deployments use rolling updates with zero downtime.
- **Database:** Multi-availability zone deployment with automatic failover to a standby replica.

- **Health monitoring:** Automated health checks run continuously. Application errors are tracked and alerted in real-time.
- **Uptime:** The platform is accessible 24/7, year-round, including out of season. Planned maintenance is scheduled outside peak usage hours and typically results in no user-facing downtime due to rolling deployments.

Headfirst has been operating continuously since 2022 with no significant service outages.

10. Incident Response

In the event of a security incident:

- The incident is identified and contained.
- Affected parties are notified within 72 hours, in line with the Notifiable Data Breaches (NDB) scheme.
- Root cause analysis is conducted and remediation applied.
- Preventive measures are implemented and documented.

To report a security concern, contact hello@headfirstapp.com.

11. Sub-processors

Headfirst uses the following third-party services to operate the platform:

- **Amazon Web Services (AWS):** Infrastructure, database, storage, backups in Sydney & Melbourne, Australia
- **Postmark:** Transactional email delivery (invitations, report emails) in United States
- **Sentry:** Application error monitoring (no user PII) in United States
- **Apple App Store / Google Play Store:** Mobile app distribution in Australia and UK

All sub-processors are subject to their own privacy and security commitments. Transactional emails sent via Postmark contain only the minimum information necessary (recipient email, invitation details, or report summary).

12. Version History

- Version 1.0: 26 March 2026 - Initial release
- Version 1.1: 27 March 2026

For questions about this document, contact hello@headfirstapp.com.