SilVR Adventures

Privacy & Security Overview

How SilVR Pathways Protects Your Participants' Data

Australian Data Storage | Privacy Act 1988 Aligned

Version 1.0 | February 2026

At a Glance

SilVR Pathways is built with privacy at its foundation, not as an afterthought. Every design decision — from the data we collect to the way we isolate organisations — prioritises the safety and dignity of participants. Our platform stores only the minimum personal information needed to deliver personalised VR experiences, enforces strict organisation-level data isolation at the database engine layer, and maintains a comprehensive audit trail of over 40 tracked action types.

Trust at a Glance

PRIVACY

Minimal PII by Design

Only first name and last initial stored. No full surnames, addresses, or medical data.

ISOLATION

Database-Level Isolation

Engine-enforced organisation data separation — not application code.

AUDIT

40+ Audited Action Types

Every sensitive operation logged with timestamps, IP, and browser details.

STORAGE

Australian Data Storage

All participant data stored on Australian-hosted infrastructure.

DELETION

Data Obfuscation on Deletion

Aggressive obfuscation across all data points. Only anonymised shells retained.

COMPLIANCE

Privacy Act 1988 Aligned

Designed to support APPs and Aged Care Quality Standard 8.

Minimal Personal Information

SilVR Pathways collects only the bare minimum personal information needed to create personalised VR plans. We store a participant's first name and last initial — nothing more. No full surnames, no home addresses, no Medicare numbers, and no medical diagnoses ever enter our system.

> Even in the unlikely event of a data breach, a record of "Margaret M. who enjoys gardening and classical music" cannot be meaningfully linked to a specific individual without external context.

What we store:

- First name — used to personalise the VR plan and address the participant during sessions.
- Last initial — a single uppercase letter (e.g., "M.") to distinguish participants with the same first name.
- Preferences and interests — hobbies, favourite destinations, cultural background used by our AI engine.
- Content avoidances — safety-critical information (e.g., fear of heights) used to exclude unsuitable content.

What we explicitly do not store:

- Full surnames or family names
- Residential addresses or room numbers
- Medicare, health insurance, or government ID numbers
- Medical diagnoses, medications, or clinical notes
- Photographs or biometric data
- Next-of-kin or emergency contact details

Organisation Data Isolation

Every organisation's data is completely isolated from every other organisation. This isolation is enforced at the database engine layer — meaning it is physically impossible for one organisation to access another organisation's participants, plans, or session data, regardless of any application-level errors.

> The security boundary exists at the infrastructure layer, independent of application code. Even a coding error cannot leak data across organisations.

How it works:

Our database uses row-level security policies — rules enforced by the database engine itself, not by application code. Every query is automatically scoped to the authenticated organisation's data.

- An organisation can only read, create, update, or delete their own participants.
- Session data, VR plans, and analytics are all scoped to the originating organisation.
- Cross-organisation queries are rejected by the database engine before they execute.

This is a fundamentally stronger isolation model than application-level filtering, where a coding error could expose data.

Secure Authentication

SilVR Pathways uses secure authentication mechanisms to protect access at every level. All credentials are cryptographically hashed before storage — they are never stored in plain text. Failed login attempts are rate-limited to prevent brute-force attacks, and every authentication event is recorded in the audit trail.

- Cryptographic credential hashing — all credentials hashed using bcrypt with a cost factor of 12 (~250ms per hash), making brute-force attacks computationally infeasible. Hashing is one-way — original credentials cannot be recovered.
- Rate limiting — failed authentication attempts trigger progressive delays and temporary blocking to prevent automated attacks.
- Secure sessions — session tokens stored in HTTP-only, secure cookies that cannot be accessed by client-side scripts.
- Instant revocation — administrators can instantly deactivate an organisation, immediately revoking all access.
- Full audit trail — every login attempt, session creation, and authentication event is logged with timestamps, IP addresses, and device information.

Content Safety Filters

Our AI-powered recommendation system places participant safety above all else. Hard safety filters override any AI recommendation, ensuring participants are never shown content that could cause distress.

> **The guiding principle: safety over recommendations. Hard filters cannot be overridden by the AI or by staff.**

Three-stage safety pipeline:

1. Hard Filters (Safety-Critical) — the participant's avoidance profile is parsed into structured safety filters. Any content matching these avoidances is immediately excluded, regardless of AI scoring.
2. Preference Scoring — remaining content is scored against the participant's interests with weighted categories.
3. AI Final Selection — our AI engine makes the final selection, ensuring diversity and generating human-readable reasoning for each recommendation.

Key safety features:

- Hard filters cannot be overridden by the AI or by staff.
- Negative-keyword detection correctly parses "not afraid of heights" as no filter needed.
- Every plan records the number of items excluded by safety filters for audit purposes.
- Only vetted, appropriate content enters the system.

Cryptographic Security

SilVR Pathways uses industry-standard cryptographic algorithms to protect sensitive data at rest and in transit. Credentials are never stored in plain text, authentication tokens are encrypted, and data integrity is verified using cryptographic signatures.

- AES-256-GCM Encryption — symmetric encryption providing both confidentiality and integrity verification. The 256-bit key length is approved for protecting classified information by the Australian Signals Directorate.
- bcrypt Credential Hashing (12 rounds) — one-way hashing making brute-force attacks computationally infeasible (~250ms per hash).
- SHA-256 Integrity Verification — tamper detection for authentication tokens and data payloads.
- Schema Validation — all data validated against strict schemas at the boundary, preventing injection attacks and data corruption.
- HTTPS/TLS — all data in transit encrypted. No unencrypted connections accepted.

Data Deletion & Obfuscation

When a participant is removed from SilVR Pathways, we aggressively obfuscate all personal information across every data point in the system. Only the anonymised record shell and audit trail are retained for compliance.

> Deletion is irreversible. All personally identifiable information is permanently removed across every data point. Only anonymised record shells and the audit trail are retained for regulatory compliance.

Participant Record:

- First name replaced with "Deleted", last initial with "X" resulting in "Deleted X."
- Every personal data field (preferences, interests, avoidances, cultural information) set to null.

AI-Generated Plans:

- All name occurrences replaced with generic placeholder text (case-insensitive matching).
- Possessive forms similarly replaced. AI reasoning text scrubbed.

PDF Documents:

- All stored PDF documents permanently destroyed (hard delete — irrecoverable).

What is retained (for compliance only):

- Anonymised record shell for referential integrity, audit trail for regulatory compliance, and aggregate statistics containing no PII.

Archive vs Delete:

- Archive — record hidden, all data preserved and restorable.
- Delete — full obfuscation across all data points; irreversible.

Comprehensive Audit Trail

Every sensitive action in SilVR Pathways is automatically logged to a tamper-resistant audit trail. With over 40 tracked action types, the audit system captures who did what, when, and from where.

Each audit entry captures:

- Precise timestamp (stored UTC, displayed AEST/AEDT)
- Action type (one of 40+ categorised types)
- Resource type and ID of the affected record
- User identifier
- Originating IP address (proxy-aware resolution)
- Browser/device user agent

Audited action categories:

Participant Operations

View, create, update, archive, unarchive, delete, bulk operations, import

Plan Operations

View, generate, download PDF, export, feedback, batch generation

Authentication Events

Login, logout, session creation, credential updates, access revocation

Session Operations

Start, end, add notes, view, export sessions

Admin Operations

Organisation management, content sync, user management

Report & Subscriptions

Generate, download, manage subscriptions

> The audit system is non-blocking — if a log write fails, the primary operation proceeds normally. Security through observability, without compromising availability.

Data Storage & Processing

All SilVR Pathways data — including participant information, VR plans, session records, and audit logs — is stored on Australian-hosted infrastructure. Some processing, such as AI-powered recommendations, may involve overseas services, but only minimal, non-identifying data is sent for processing.

- Database storage — all participant data stored in Australian data centres. Stored data never leaves Australia.
- Application hosting — Australian infrastructure.
- AI processing — our AI engine, used to generate personalised VR plans, may process data on infrastructure located outside Australia. However, only minimal information is sent: first name, last initial, and lifestyle preferences. No full names, addresses, medical data, or other sensitive information is ever sent to external services.
- Content delivery — VR content metadata served from Australian infrastructure. VR content files are managed on the organisation's headset devices.

Regulatory Alignment

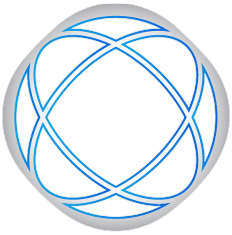
SilVR Pathways is designed to support compliance with the Australian Privacy Act 1988, the Australian Privacy Principles (APPs), and the Aged Care Quality Standards.

Australian Privacy Act 1988 & APPs:

Principle	How SilVR Pathways Supports It
APP 1 — Open & transparent	This document, clear data practices, audit trail
APP 3 — Collection	Minimal PII — only what's necessary for VR personalisation
APP 6 — Use or disclosure	Data used solely for VR plans; organisation isolation prevents cross-disclosure
APP 8 — Cross-border	Data stored in Australia; only minimal, non-identifying data may be processed overseas for AI
APP 11 — Security	AES-256-GCM, bcrypt, database-level isolation, audit trail
APP 12 — Access	Staff can view all participant data; plans downloadable as PDFs
APP 13 — Correction	Participant profiles fully editable by authorised staff

Aged Care Quality Standard 8 — Organisational Governance:

- Information governance — audit trail evidences responsible data handling
- Risk management — safety-first content filtering protects participants
- Privacy protection — minimal PII and database-level isolation
- Continuous improvement — session feedback and analytics support quality improvement



SilVR Adventures

For more information about our privacy and security practices, contact us at:

hello@silvradventures.com.au

pathways.silvradventures.com.au

SilVR Pathways — Personalised VR Experiences

Privacy & Security Overview v1.0 | February 2026

Australian Data Storage | Privacy Act 1988 Aligned