Waylight Pty Ltd

Waylight Plan Management

Document Title	Information Management Policy
Document Number	WL-POL-13
Version	1.0
Date	2026-04-02
Review Date	2027-04-02
Approved By	Joshua, Director
Classification	Internal

1. Purpose

This policy establishes Waylight's framework for collecting, using, storing, securing, and disposing of participant and business information. Waylight handles sensitive personal and financial information as a plan manager. This policy ensures compliance with Commonwealth and Queensland privacy legislation and the NDIS Practice Standards.

2. Scope

This policy applies to all workers, contractors, and volunteers engaged by Waylight Pty Ltd in the delivery of plan management services. It covers all participant information, worker information, and business records held by Waylight.

3. Applicable Standards

- NDIS Practice Standards, Verification Module, Information Management: Documented system for information management in place.
- Privacy Act 1988 (Cth). Australian Privacy Principles.
- Information Privacy Act 2009 (QLD).
- NDIS Code of Conduct. Element 3: Provide supports and services in a safe and competent manner with care and skill (includes protecting participant information).

4. Policy Statement

- Waylight collects only the personal information necessary to deliver plan management services.
- Participant information is collected with the participant's informed consent.
- Information is stored securely in Waylight's digital management system (Supabase, hosted in Sydney region) with appropriate access controls.
- Information is used only for the purpose for which it was collected, unless required by law.
- Participants can access, correct, and request deletion of their personal information.

- Records are retained for the legally required period and securely destroyed thereafter.

5. Procedure

5.1 Collection

- Step 1: Waylight collects participant information necessary for plan management: name, date of birth, NDIS number, contact details, NDIS plan details (support categories and budgets), service provider details, and invoices.
- Step 2: Participants are informed at sign-up (via the Service Agreement) about what information is collected, why, how it is stored, who has access, and their rights.
- Step 3: Consent is obtained at the point of collection. Participants can withdraw consent at any time, this may affect Waylight's ability to provide services.

5.2 Storage and Security

- All participant and financial data is stored in Supabase (Sydney region) with: encryption at rest and in transit, role-based access controls, automated backups, and audit logging.
- Access is restricted to the Director and Contractor-Accountant. Future workers receive access only to the data necessary for their role.
- Passwords are unique, complex, and stored in a password manager. Multi-factor authentication is enabled where available.
- Physical documents (if any) are stored in a locked cabinet at the Director's home office.

5.3 Use and Disclosure

- Participant information is used only for: processing invoices and lodging claims, tracking budgets, communicating with participants about their plan, and reporting as required by the NDIS Commission.
- Information is not disclosed to third parties except: to service providers as necessary to process claims (provider name and invoice details), to the NDIA/NDIS Commission as required by legislation, with the participant's explicit consent, or as required by law.

5.4 Participant Access and Correction

- Participants can request access to their personal information held by Waylight at any time. Waylight responds within 10 business days.
- If information is inaccurate, the participant can request correction. Waylight corrects errors within 5 business days.
- If a participant requests deletion of their data and no legal retention obligation applies, Waylight securely deletes the data within 30 business days.

5.5 Retention and Destruction

- Financial records: retained for 7 years from the date of the transaction.

- Incident records: retained for 7 years from the date the record is made.
- Complaint records: retained for 7 years from the date the record is made.
- Worker screening records: retained for the duration of engagement plus 7 years.
- General participant records: retained for the duration of the service agreement plus 7 years.
- After the retention period, digital records are securely deleted. Physical records (if any) are shredded.

5.6 Data Breach Response

- If a data breach is identified (unauthorised access, loss, or disclosure of participant information): Step 1: contain the breach immediately, Step 2: assess the breach (what data, who affected, likely harm), Step 3: notify affected participants within 48 hours, Step 4: if the breach meets the threshold under the Privacy Act, notify the Australian Information Commissioner, Step 5: document the breach and remedial actions taken.

6. Responsibilities

Role	Responsibility
Director (Joshua)	Implements information management controls. Manages access permissions. Responds to participant access/correction requests. Manages data breach response.
Contractor-Accountant	Accesses financial data only as needed for reconciliation. Complies with information security procedures.
Plan Management Worker (future)	Accesses only data necessary for their role. Complies with information security procedures. Reports potential breaches immediately.
Participants	Provide consent for data collection. Request access or correction of their information. Report any suspected breaches.

7. Related Documents

- WL-POL-05 Participant Service Agreement (privacy section)
- Privacy Act 1988 (Cth)
- Information Privacy Act 2009 (QLD)
- NDIS Practice Standards (Verification Module)

8. Audit Readiness Notes

- Q: 'How is participant information stored and secured?', A: All data is in Supabase, hosted in Sydney. Encrypted at rest and in transit. Role-based access, only the Contractor-Accountant and I have access. Automated backups. Audit logging tracks who accessed what.

- Q: 'What happens if there is a data breach?'. A: Contain immediately, assess the scope, notify affected participants within 48 hours, notify the Australian Information Commissioner if the threshold is met, document everything and take remedial action.
- Q: 'Can a participant access their records?'. A: Yes. They request it and I provide it within 10 business days. If anything is wrong, I correct it within 5 business days.

9. Review

This policy is reviewed annually or earlier if there are changes to privacy legislation, NDIS requirements, or organisational operations. Next scheduled review: 2027-04-02.

Version History

Version	Date	Author	Changes
1.0	2026-04-02	Joshua	Initial version
1.1	2026-04-02	Joshua	POLISH: Added Notifiable Data Breaches scheme threshold reference (Privacy Act Part IIIC).