Privacy Policy

NDIS Plan Management Provider — OPM 18.01.15

Document title	Privacy Policy
Document number	OPM 18.01.15
Supersedes	Privacy Policy v3.0 (13 July 2026)
Applies to	Orange Plan Management, its workers, and all individuals whose personal information OPM collects and handles, including participants, their representatives, providers, visitors and OPM workers
Related standards	Privacy Act 1988 (Cth) and Australian Privacy Principles; Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth); NDIS Act 2013 (Cth) s 60; NDIS (Protection and Disclosure of Information) Rules 2013; NDIS (Provider Registration and Practice Standards) Rules 2018; NDIS (Quality Indicators for NDIS Practice Standards) Guidelines 2018; NDIS Code of Conduct
Policy owner or Author	Compliance & HR Manager (owner); Author: Rehan Lowmass (Director)
Approved by	Patricia Lowmass (Compliance & HR Manager)
Version	3.1
Date approved	24 September 2026
Next review date	September 2028 (or earlier if legislation changes)

1. Purpose

This policy ensures that Orange Plan Management (OPM) protects and handles personal information in accordance with the NDIS and relevant privacy legislation. OPM acknowledges an individual's right to privacy while recognising that personal information is required to be collected, maintained and administered to provide a safe working environment and a high standard of quality.

The information collected is used to provide services to participants in a safe and healthy environment with individual requirements, to meet duty of care obligations, to initiate appropriate referrals, and to conduct business activities to support those services.

2. What Information May Be Collected

As a NDIS Plan Manager, we collect and use personal information so we can provide plan management services, process invoices, support budget tracking, communicate with you and your providers, and meet our legal and regulatory obligations.

OPM may collect the following types of personal and sensitive information:

- your name, date of birth and contact details
- your NDIS number
- details about your NDIS plan, funding and budgets

- nominee, guardian, carer or support coordinator details
- provider details
- invoices, service agreements and claim information
- payment and banking-related information where required
- records of phone calls, emails, SMS messages or other communications
- feedback, complaints or incident-related information
- information needed to verify identity or authority to act on your behalf

OPM will only collect information that is reasonably necessary to carry out our functions and activities as a NDIS Plan Manager. Information about OPM workers is covered in section 10.

3. Regulations Relevant to This Policy

The NDIS Code of Conduct requires providers and workers to respect the privacy of people with disability, and the NDIS Practice Standards include expectations around respecting and protecting participant privacy and dignity.

- NDIS (Provider Registration and Practice Standards) Rules 2018 (Cth)
- Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)
- NDIS (Quality Indicators for NDIS Practice Standards) Guidelines 2018 (Cth)
- Privacy Act 1988 (Cth) and the Australian Privacy Principles
- NDIS Act 2013 (Cth) s 60 — protection of information held for the purposes of the NDIS
- NDIS (Protection and Disclosure of Information) Rules 2013

4. How OPM Collects Information

- Directly from the Participant or Representative via intake forms, phone calls, emails, or meetings
- From authorised representatives, guardians, or nominees
- Through the NDIS portal
- From service providers or support coordinators, where relevant and with consent

We may also collect information from other people or organisations involved in your supports, including:

- your nominee, guardian, family member or authorised representative
- support coordinator or recovery coach
- service providers
- the NDIA
- other NDIS-related systems or portals
- auditors, regulators or professional advisers, where required

Where possible, we will collect information directly from you. If information is collected from someone else, we will take reasonable steps to make sure you know about it. We may also collect sensitive information, such as information about your disability, health, support needs or services received, but only where it is required for us to provide plan management services or comply with the law.

Visitors to our office sign the Visitor Register. Their details are collected for security and safety purposes and are retained for 12 months, then securely destroyed, under the Physical Security Policy (including Visitor Register) (OPM 18.01.35).

5. Why We Collect, Use and Disclose Personal Information

We collect, use and disclose personal information so we can:

- provide NDIS plan management services
- process and pay invoices
- submit claims through the NDIS
- track your NDIS budgets and spending
- communicate with you, your representatives and your providers
- respond to enquiries, feedback and complaints
- keep accurate business and service records
- meet audit, quality, safeguarding and regulatory requirements
- prevent, detect or respond to fraud, misuse of funds or payment errors
- comply with legal obligations

We will not use or disclose your personal information for a purpose unrelated to our services unless:

- you have given consent
- it is required or authorised by law
- it is necessary to prevent or respond to a serious risk to health, safety or wellbeing
- it is required for an audit, investigation, complaint, safeguarding matter or regulatory process

NDIS guidance states that providers are not authorised to use or disclose participant information for purposes other than the intended purpose.

6. Who We May Share Information With

We may share relevant information with:

- you and your authorised representatives
- your service providers
- your support coordinator, recovery coach or other support contacts
- the NDIA
- the NDIS Quality and Safeguards Commission
- auditors or quality assessors
- payment processors, accounting systems or software providers
- IT, cloud storage, cybersecurity and business support providers
- legal, insurance or professional advisers
- government agencies, courts or regulators where required by law

We only share the information needed for the relevant purpose.

7. Privacy and Confidentiality Guidelines

To support the privacy and confidentiality of individuals, OPM ensures:

- we are committed to complying with the privacy requirements of the Privacy Act 1988 (Cth), the Australian Privacy Principles and the Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth) as required by organisations providing disability services

- we are fully committed to complying with the consent requirements of the NDIS Quality and Safeguarding Framework and relevant state or territory requirements
- we provide all individuals with access to information about the privacy of their personal information; this information is also available as Your Privacy — Easy Read (OPM 18.02.18), and in other formats or languages on request
- everyone has the right to opt out of consenting to and providing their personal details if they wish
- individuals have the right to request access to their personal records by requesting this with their contact person
- where we are required to report to government funding bodies, information provided is non-identifiable and related to services and support hours provided, age, disability, language, and nationality
- personal information will only be used by us and will not be shared outside the organisation without your permission unless required by law (e.g. reporting assault, abuse, neglect, or where a court order is issued)
- images or video footage of participants will not be used without their consent; consent for the use of a participant's image, story or testimonial is specific, in writing and recorded on the participant's file (OPM 18.01.41)
- participants have the option of being involved in external NDIS audits if they wish.

OPM will seek your consent before sharing your information where consent is required, and records it on the Consent to Release Information Form (OPM 18.02.03). You may choose who we can communicate with about your plan management services. This may include family members, nominees, guardians, support coordinators or providers.

You can withdraw or change your consent at any time by contacting us. However, this may affect our ability to provide some services. A participant's refusal or withdrawal of consent is recorded on their file and respected, and is never a reason to treat the participant less favourably (Decision-Making, Capacity and Consent Policy, OPM 18.01.41).

You have the right to ask for access to the personal information we hold about you. You can also ask us to correct information if it is inaccurate, out of date, incomplete or misleading.

To request access or correction, contact us using the details at the end of this policy. We may need to verify your identity before providing access or making changes. We will respond within a reasonable timeframe.

8. Security of Information

To keep information secure, OPM ensures:

- we take reasonable steps to protect the personal information we hold against misuse, interference, loss, unauthorised access, modification and disclosure
- we ensure personal information is accessible to the participant and is able for use only by relevant workers
- we ensure security for personal information includes password protection for IT systems, with only authorised personnel permitted access
- we ensure personal information no longer required is securely destroyed or de-identified.

Our privacy and security measures may include:

- secure client management and accounting systems
- password protection and multi-factor authentication
- restricted staff access based on role and need

- staff training on privacy and confidentiality
- secure document storage
- secure email and communication practices
- regular review of access permissions
- processes for managing suspected data breaches
- secure disposal or de-identification of information when no longer required

OPM uses approved artificial intelligence (AI) tools only in accordance with the Responsible and Secure Use of AI Policy (OPM 18.01.37), and workers do not enter participant information into any AI tool that has not been approved under that policy.

OPM will keep personal information for as long as needed to provide services, meet legal obligations, respond to disputes, comply with audits, and maintain accurate business records, in line with the retention schedule in the Records and Information Management Policy (OPM 18.01.32).

When information is no longer required, we will take reasonable steps to securely destroy or de-identify it, unless we are required by law to keep it.

9. Data Breaches

As part of information security responsibilities, OPM ensures:

- we will take reasonable steps to reduce the likelihood of a data breach occurring including storing personal information securely and accessible only by relevant workers
- if we know or suspect your personal information has been accessed by unauthorised parties, and we think this could cause you harm, we will take reasonable steps to reduce the chance of harm and advise you of the breach, and if necessary, the Office of the Australian Information Commissioner.

A data breach may occur if personal information is lost, accessed, disclosed or used without authorisation. Examples include:

- sending an email to the wrong person
- unauthorised access to a participant file
- loss or theft of a device containing personal information
- cyber incidents affecting business systems

If a data breach occurs, we will act promptly to contain the breach, assess the risk, notify affected people where appropriate, and comply with any reporting obligations under the Notifiable Data Breaches scheme (see the Data Breach Response & Notification Plan, OPM 18.01.07).

10. Worker Personal Information

OPM collects and holds personal and sensitive information about its workers — employees, contractors, volunteers, students and job applicants. This section explains how that information is handled. It is read with the Worker Screening and Induction/Onboarding Policy (OPM 18.01.25), the Staff Performance Management Policy (OPM 18.01.19) section 11 and the Records and Information Management Policy (OPM 18.01.32).

10.1 What we collect

- identity documents and contact details
- evidence of the right to work in Australia

- NDIS Worker Screening clearance and verification records and, where a role requires it, Working with Children Check records
- qualifications, professional memberships and CPD evidence
- emergency contact details
- health information relevant to work health and safety, workplace adjustments or leave, collected with the worker's consent or where the law requires it
- payroll, taxation and superannuation details
- performance, training, grievance and disciplinary records

10.2 Why we collect it

Worker information is collected to assess a person's suitability for a role, meet NDIS worker screening and qualification requirements, pay workers and meet tax and superannuation obligations, meet work health and safety obligations, manage performance and development, and evidence OPM's compliance with the NDIS Practice Standards and its conditions of registration.

10.3 Who we disclose it to

Worker information is disclosed only as needed for those purposes, including to:

- the NDIS Worker Screening Database, to verify and monitor a worker's clearance
- the Australian Taxation Office and the worker's superannuation fund
- WorkCover Queensland, where a workers' compensation claim is made
- the NDIS Commission or OPM's approved quality auditor, as evidence of compliance — de-identified or sampled where that meets the purpose
- OPM's payroll and accounting service providers, under confidentiality obligations
- any other person where the worker consents or the law requires it

10.4 How we secure and retain it

Worker records are held on personnel files in a restricted SharePoint location. Access is limited to the Compliance & HR Manager, the General Manager and the Directors. Worker records are kept for 7 years after the worker's engagement with OPM ends, then securely destroyed, under the Records and Information Management Policy (OPM 18.01.32).

10.5 Access and correction

A worker may ask the Compliance & HR Manager to access or correct the personal information OPM holds about them. The Compliance & HR Manager responds within a reasonable time and records the request on the worker's personnel file. Although the Privacy Act 1988 (Cth) contains an exemption for employee records held by an employer, OPM applies the standards in this policy to all worker personal information as good practice, and employees may also inspect and copy their employee records as the Fair Work Regulations 2009 allow.

11. Website and Online Information

If you use our website, we may collect limited technical information such as your IP address, browser type, device information and pages visited. We may use cookies or analytics tools to improve our website and services. If you submit information through an online form, we will use that information to respond to your enquiry or provide the service requested.

12. Complaints About Privacy

If you have a concern or complaint about how we have handled your personal information, please do not hesitate to get in touch with us at feedback@orangeplan.com.au or by calling 1300 611 990. We will acknowledge your complaint and aim to respond within a reasonable timeframe.

If you are not satisfied with our response, you may contact the Office of the Australian Information Commissioner. You may also raise concerns with the NDIS Quality and Safeguards Commission where the matter relates to NDIS provider conduct, participant rights, privacy, dignity, safety or quality of supports.

13. Related Documents

- Your Privacy — Easy Read (OPM 18.02.18); Consent to Release Information Form (OPM 18.02.03)
- Decision-Making, Capacity and Consent Policy (OPM 18.01.41)
- Records and Information Management Policy (OPM 18.01.32); Data Security Policy (OPM 18.01.08); Data Breach Response & Notification Plan (OPM 18.01.07)
- Responsible and Secure Use of AI Policy (OPM 18.01.37); Physical Security Policy (including Visitor Register) (OPM 18.01.35); Visitor Register (10.0 Risk Management & Compliance Registers/01. Risk Registers)
- Staff Performance Management Policy (OPM 18.01.19); Worker Screening and Induction/Onboarding Policy (OPM 18.01.25)
- Complaint Handling Policy and Procedure (OPM 18.01.04)
- Documents that reference this policy and are read with it: Participant Rights and Safeguards Policy (OPM 18.01.14); Remote Working and Working from Home Policy (OPM 18.01.17); Whistleblower Policy (OPM 18.01.23); Ongoing Professional Development Policy (OPM 18.01.31); Infection Prevention and Control Policy (OPM 18.01.33); Acceptable Use Policy (including Social Media) (OPM 18.01.34); Confidentiality Agreement Process (OPM 18.01.38); Plan Management Enquiry Escalation Procedure (OPM 18.01.40); Child Safe Policy (OPM 18.01.42); Participant Entry, Exit and Transition Policy (OPM 18.01.43); Advocacy Policy (OPM 18.01.47)

14. Policy Review

We will update this Privacy Policy to reflect changes in our business operations or services, as follow up to an internal incident or investigation indicating a need for improvement in our systems, or due to legal obligations or legislative or regulatory requirements. The latest version will be available on our website or by contacting us.

This policy will be reviewed in September 2028 or following any relevant legislative or practice changes. Review responsibility sits with the Compliance & HR Manager.

Contact Us

If you have a question about this policy, please contact us at feedback@orangeplan.com.au or by calling 1300 611 990.

Our address is Unit 3A, 11 Donkin St, West End QLD 4101. NDIS Provider 4050021671.

Document Version History

Version	Date	Summary of changes	Author
1.0	19 June 2025	OPM specific policy	Patricia Lowmass
2.0	28 April 2026	Updated with examples of OPM privacy & security measures and data breaches; Complaints about privacy information added	Patricia Lowmass
3.0	13 July 2026	Reformatted to OPM standard policy format; document control updated	Patricia Lowmass
3.1 DRAFT	23 September 2026	Worker information, visitor, consent, AI and retention provisions added; role title updated.	Rehan Lowmass (Director)
3.1	24 September 2026	Approved and made live.	Patricia Lowmass (Compliance & HR Manager)