



NDIS Quality
and Safeguards
Commission

Privacy Policy

Version 4.2

August 2026



**NDIS Quality
and Safeguards
Commission**

NDIS Quality and Safeguards Commission

PO Box 210, Penrith NSW 2751

Copyright

© Commonwealth of Australia (NDIS Quality and Safeguards Commission) 2024



The NDIS Quality and Safeguards Commission encourages the dissemination and exchange of information provided in this policy. The material in this policy is licensed under a Creative Commons Attribution 4.0 International licence, with the exception of:

- the Commonwealth Coat of Arms
- the NDIS Quality and Safeguards Commission logo
- any material protected by or used as a trade mark
- any third party material, including any illustration, diagram, photograph or graphic over which the NDIS Quality and Safeguards Commission does not hold copyright, but which may be part of or contained within this policy.

More information on this CC BY licence is set out at the creative commons website: www.creativecommons.org. Enquiries about this licence and any use of this policy can be sent to: communications@ndiscommission.gov.au

Attribution

Use of all or part of these guidelines must include the following attribution:

© Commonwealth of Australia (NDIS Quality and Safeguards Commission) 2024.

Using the Commonwealth Coat of Arms

Terms of use for the Coat of Arms are available at this website:

<https://www.pmc.gov.au/government/commonwealth-coat-arms>

Important notice

The information in this policy is for general guidance only. It does not constitute legal or other professional advice, and should not be relied on as a statement of a law in any jurisdiction. You should obtain professional advice if you have any specific concern.

The NDIS Quality and Safeguards Commission has made every reasonable effort to provide current and accurate information, but it does not make any guarantees regarding the accuracy, currency or completeness of that information.

Parties wishing to re-publish or otherwise use the information in this policy must check this information for currency and accuracy prior to publication. This should be done prior to each publication edition, as NDIS Quality and Safeguards Commission guidance and relevant legislation may change. Any queries should be addressed to communications@ndiscommission.gov.au.

Table of contents

Privacy Policy	1
Definitions.....	5
1. About this Privacy Policy	7
Purpose	7
Other legislation	7
2. What information we collect.....	8
Personal information	8
Sensitive information.....	9
3. How we collect information	9
4. Artificial Intelligence (AI) transparency	10
5. Anonymity and pseudonymity	11
6. How we store and secure personal information.....	11
Shared services	12
7. Responding to data breaches.....	12
8. Use and disclosure of personal information	12
Use of personal information.....	12
Disclosure of personal information	13
Data sharing and matching	14
9. Disclosure of personal information to overseas recipients	14
10. Quality, access, and correction	14
11. Online interactions	15
Our website.....	15
Cookies.....	15
Third party websites	16
Email addresses	16
Electronic newsletters or subscriptions.....	16
12. Feedback and complaints.....	16
How to contact the NDIS Commission.....	16
How to complain to the OAIC	17
13. How to contact us.....	17
Request a copy of the Privacy Policy, submit a query or make a complaint	17
Contact details for freedom of information (FOI) requests.....	17

14.	NDIS Commission Personnel	17
15.	Key appointments and roles.....	18
	Privacy Champion	18
	Privacy Officers	18
16.	Personnel responsibilities.....	19
17.	Further information.....	19
	Privacy Impact Assessments	19
	Privacy guidance	20



Definitions

The meaning of key terms and abbreviations in this procedure are set out in the table below.

Term or Abbreviation	Description
AI	Artificial Intelligence
Data breach	When personal information that an entity holds is subject to unauthorised access or disclosure, or is lost (source: Part 1: Data breaches and the Australian Privacy Act OAIC)
De-identification	A privacy enhancing process that reduces the risk of an individual being identified or re-identified in data (source: De-identification and the Privacy Act Office of the Australian Information Commissioner)
Disclosure	Give access to, or show information to an individual, organisation, or the public.
Information	Data, information and records in any format, whether analogue or digital (source: National Archives of Australia). The terms 'information' and 'data' are often used interchangeably. In some contexts, data may be considered to be a subset of information. Some legislation refers to data and some legislation refers to information. This Privacy Policy uses both terms as may be relevant to the context.
LLM	Large Language Model
NDIS Act	The National Disability Insurance Scheme Act 2013
Personal information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not. Personal information is a subset of protected Commission information (source: section 6, Privacy Act 1988 and NDIS Commission Privacy Policy).
Privacy Act	means the <i>Privacy Act 1988 (Cth)</i> .

Personnel	Personnel means all persons employed or otherwise engaged by the NDIS Commission, including any volunteers or contractors.
Protected Commission information	Information about a person (including a deceased person) that is or was held in the records of the NDIS Commission, excluding information published in the NDIS Provider Register. ‘Person’ includes an individual, a body corporate or body politic. It is an offence to collect, use or disclose protected Commission information except as authorised under the NDIS Act. The provisions that govern protected Commission information are sometimes referred to as ‘secrecy provisions’ (source: section 9 and chapter 4 part 2, NDIS Act).
Sensitive information	A subset of personal information that requires greater protection under the Privacy Act 1988. Includes information or an opinion about an individual’s religious beliefs or affiliations, political opinions or membership, racial or ethnic origin, philosophical beliefs, sexual orientation or practices, criminal history, health information, genetic information, biometric information or templates. Sensitive information is a subset of personal information (source: section 6, Privacy Act 1988).

1. About this Privacy Policy

The NDIS Quality and Safeguards Commission (NDIS Commission) must comply with the Australian Privacy Principles (APPs) contained in Schedule 1 of the [Privacy Act 1988 \(Cth\)](#) (Privacy Act). The APPs set out standards, rights and obligations around personal information. The NDIS Commission also has privacy obligations under the [Privacy \(Australian Government Agencies - Governance\) APP Code 2017](#) (Privacy Code).

The NDIS Commission will update this Privacy Policy when its personal information handling practices change. Updates made to this Privacy Policy are made accessible on the NDIS Commission website.

Purpose

The NDIS Commission recognises the importance of protecting personal information entrusted to us by NDIS participants, their nominees/representatives, sector workers and other members of the public. Information provided to the NDIS Commission, including personal information assists the NDIS Commission to exercise its powers and functions as a regulator, and maintain robust sector oversight.

This Privacy Policy provides information about how the NDIS Commission collects, uses, discloses and holds personal information and how individuals may access and correct the personal information we hold about them.

The Privacy Policy applies to:

- personal information collected, used, disclosed and stored by the NDIS Commission, and
- all Personnel, including contractors and consultants engaged by the NDIS Commission.

This Privacy Policy does not cover non-personal information management related to:

- a body corporate/politic or business record
- data retention or integration practices, or
- cybersecurity measures.

Other legislation

In addition to our obligations under the Privacy Act, the NDIS Commission must also handle 'protected Commission information' in accordance with the secrecy provisions in the *National Disability Insurance Scheme Act 2013* (Cth) (NDIS Act). Generally, all personal information held by the NDIS Commission falls within the definition of 'protected Commission information.'

Unauthorised use and disclosure of protected Commission information by any person is a criminal offence under the NDIS Act. The NDIS Commission also requires its contracted service providers to comply with these legal requirements.

2. What information we collect

The NDIS Commission only collects personal information to exercise and perform its functions under the NDIS Act. As the regulator of the NDIS, some of the NDIS Commission's core functions include:

- provider registration
- complaints
- reportable incidents
- engagement, education and communications
- compliance and enforcement
- worker screening
- market and regulatory oversight and risk

The personal information we collect is reasonably necessary for, or directly related to our functions or activities, or when required to do so by law. We collect personal information when:

- you apply for registration as an NDIS provider
- we undertake compliance and enforcement activities or investigations
- we receive and assess complaints
- you request access to resources, training and education sessions, or ask to be placed on a mailing list
- we consult with stakeholders, or carry out data analytics and sector research
- you apply to be a behaviour support practitioner
- we perform recruitment and employment processes, contractors and service providers
- we provide subscription services or information access made under the *Freedom of Information Act 1982* (Cth) (FOI Act)

Personal information

Personal information is information or an opinion about an identified individual or an individual who is reasonably identifiable. The types of personal information we collect varies depending on what we need to perform our functions and activities and may include:

- contact details (such as your name, address, email and telephone numbers)
- biographical data (such as your date of birth (DOB) and gender)
- employment status and history (such as previous employment, work history, referee comments, remuneration)
- education status
- financial information (such as bank details, payment details, and information about business and financial interests)
- government identifiers (such as Centrelink and Medicare Reference Numbers, Tax File Number)

-
- information about your family and other related persons (such as any partners, children, dependants, carers or nominees or authorised representatives)
 - information about your personal circumstances (e.g. marital status, age, gender, occupation)
 - feedback, complaints or application related information
 - information about the supports and services you have provided to NDIS participants and how you provided those supports and services

Sensitive information

We may collect sensitive information about you if you consent and the collection is reasonably necessary for, or directly related to, one or more of our functions or activities, or the collection is required or authorised by law. The sensitive information we may collect includes:

- cultural and linguistic background (including languages you speak)
- health and disability information
- information about supports and services you receive under the National Disability Insurance Scheme (NDIS)
- criminal history
- biometrics (including photographs and video recordings)
- your identity (e.g. date of birth, country of birth, passport details, visa details, drivers' licence, birth certificates, ATM cards)

3. How we collect information

The NDIS Commission collects personal information through various means including paper and electronic forms, online portals, written correspondence, face to face and over the phone discussions and using AI tools (see further below). If it is reasonable and practical to do so, we will collect personal information directly from you or your authorised representatives.

We may also obtain your personal information collected by other Commonwealth agencies, State or Territory government bodies, other organisations, members of the public or publicly available sources for the purposes of fulfilling our regulatory functions such as:

- considering and determining the outcome of an application to be a registered NDIS provider
- responding to reportable incidents, behaviour support services or handling complaints made to us
- monitoring or investigating an NDIS provider's or worker's compliance with the NDIS Act, Rules and Code of Conduct
- taking compliance and enforcement action
- assessing applications for employment with the NDIS Commission and associated employment matters (including security and pre-employment integrity checks)

-
- assessing applications to participate in any NDIS Commission funded programs and initiatives
 - managing contracts and funding agreements, or
 - undertaking other regulatory action under the NDIS Act and the NDIS Rules.

We may collect personal information from third parties if:

- you have consented
- we are required or authorised by law to do so, or
- it would be unreasonable or impracticable to collect the personal information from you – for example, where notification could jeopardise an ongoing investigation.

When your personal information is collected, we will take reasonable steps to inform you about why the information is collected and how it will be handled. We include a privacy collection notice for specific activities either on our paper-based forms or linked to online portals that describes the reason why the information is being collected and to whom the information may be disclosed to.

The NDIS Commission may also collect personal information when you:

- visit our website
- view updates we make via other online media services, such as Meta (formerly Facebook), YouTube and survey systems.

This assists us to improve our website, identify the number visits and receive feedback from the community.

4. Artificial Intelligence (AI) transparency

The NDIS Commission may collect and process personal information using data analytics tools and AI tools, including large language models (LLMs), to perform our functions and activities more productively and efficiently (including triaging complaints, categorisation of issues, identification of patterns, and preparation of summaries or insights). This may also involve the use of personal and sensitive information for related or directly related purposes.

While these tools are used to assist us to identify insights and risks, process and analyse information and support regulatory functions, all outputs from LLMs are reviewed by our Personnel. AI tools do not make regulatory decisions or determine outcomes, as all substantive decisions are made by authorised Personnel.

AI tools may generate outputs (for example, annotations of documents) that include personal or sensitive information. This AI generated content is treated as part of the NDIS Commission's records.

The NDIS Commission monitors and evaluates its use of AI tools to ensure that collection and use of personal information including in AI outputs is appropriate, accurate and does not result in unintended impacts.

Where appropriate, the NDIS Commission provides specific privacy collection notices at the point of collection, including information about the use of AI tools and LLMs in processing personal information.

For further information about how AI is used, including governance, safeguards and oversight, please refer to the Artificial Intelligence (AI) Transparency Statement – February 2026 published by the NDIS Commission.

5. Anonymity and pseudonymity

Generally, individuals can choose to remain anonymous or adopt a pseudonym (a name, term or descriptor that is different to your actual name) when dealing with the NDIS Commission. However, in certain circumstances this might not be feasible – for example, where we need an individual's name and address to register them as an NDIS provider.

We will inform you if you are not able to remain anonymous or use a pseudonym when dealing with us or if your anonymity may impact our engagement with you.

6. How we store and secure personal information

The NDIS Commission stores personal information in a variety of formats including, but not limited to:

- hard copy files
- databases
- NDIS Commission issued devices (i.e. laptops, mobile phones, computers)
- third party storage providers such as cloud storage facilities

Personal information generated or derived using AI tools including LLMs, is stored within the NDIS Commission's secure information systems, including the Customer Relationship Management system and Data Analytics Platform.

Information generated by AI tools is treated as part of NDIS Commission's official records and may include personal or sensitive information. This information is subject to the same safeguards applied to all personal information held by the NDIS Commission in accordance with the Privacy Act.

We take reasonable steps to protect your personal information against misuse, interference, and loss, as well as from unauthorised access, modification or disclosure. These steps include:

- storing records securely as per Australian government security guidelines
- only accessing personal information on a need-to-know basis and by authorised Personnel
- monitoring system access which can only be accessed by using authenticated credentials
- regularly updating and auditing our storage and data security systems
- ensuring access to our buildings are secure at all times
- undertaking due diligence with respect to third party service providers who may have access to personal information to ensure (as far as practicable) compliance with the APPs
- ensure destruction, deletion or de-identification of personal information we hold that is no longer required to be retained by the *Archive Act 1983* (Cth) or any other applicable laws.

Shared services

The NDIS Commission works with 2 partner agencies: Services Australia (SvA) and the Department of Social Services (DSS). They provide shared information technology services and management systems. Personal information we collect may be stored in our partners' systems. They are also subject to the Privacy Act and have the same information management statutory obligations.

7. Responding to data breaches

The NDIS Commission will take appropriate, prompt action including reporting to the Office of the Australian Information Commissioner (**OAIC**) if an eligible data breach occurs and personal information we hold is subject to unauthorised modification, loss, use or disclosure.

If we suspect unlawful disclosure, access or loss has occurred, the NDIS Commission will undertake an assessment and take necessary steps to contain the breach to minimise the potential risk of harm. The NDIS Commission will determine if an 'eligible data breach' has occurred, within 30 days of being informed of the potential breach and notify the OAIC and affected persons in accordance with our Data Breach Response Plan.

8. Use and disclosure of personal information

Use of personal information

The NDIS Commission uses personal information to exercise its powers or perform its functions and duties (including complaints handling, investigations, risk assessments), and to undertake research, analytics, improvements and reporting related to its functions, as well as to progress employment opportunities. This includes use of personal information processed or generated using AI tools or LLMs.

The NDIS Commission will generally only use or disclose personal information for the purpose for which it is collected (primary purpose). Personal information may be used or disclosed for another purpose (secondary purpose), if one of the following applies:

- you have consented to the use or disclosure
- you would reasonably expect us to use or disclose the personal information for the secondary purpose because the secondary purpose is related to the primary purpose for which it was collected (or if it is sensitive information, it is directly related to the primary purpose)
- we are required or authorised by law to use or disclose the personal information
- a permitted general situation exists in relation to the use or disclosure—including where we reasonably believe that using or disclosing the information is necessary to:
 - lessen or prevent a serious threat to the life, health or safety of any individual or to public health or safety
 - take appropriate action in relation to suspected unlawful activity or serious misconduct

- establish, exercise, or defend a legal or equitable claim
- we reasonably believe the use or disclosure is necessary for our compliance or enforcement activities.

The NDIS Commission is required or authorised to collect, use or disclose personal information by a variety of laws including, though not limited to:

- NDIS Act
- *Regulatory Powers Act 2014*
- *Public Governance, Performance and Accountability Act 2013*
- *Administrative Decisions (Judicial Review) Act 1977*
- *Public Interest Disclosure Act 2013*
- *Corporations Act 2001*

If we collect personal information in the course of carrying out one of our functions and the information is relevant to another of our regulatory functions, generally we use the personal information for the related function.

Disclosure of personal information

The NDIS Commission may disclose personal information to other agencies/bodies directly related to, or reasonably necessary for its functions, including:

- lawyers and other service providers who we engage to assist us with our functions
- other Commonwealth Government agencies (such as the NDIA, and other agencies who are involved in the Fraud Fusion Taskforce)
- law enforcement bodies (including State and Territory Police and Australian Federal Police)
- State and Territory Government agencies, Coroners and regulators with a role that have a connection with NDIS supports and services
- responsible Ministers and Parliamentary committees exercising their oversight functions
- the Australian Government Security Vetting Agency or any other vetting providers that we engage to conduct security or vetting assessments on our behalf
- the public, if the personal information is required to be published on a public register, in the Government gazette or on our website (such as information published on the NDIS Provider Register)
- referees and former employers to verify qualifications and experience when assessing certain applications
- any Royal Commission whose terms of reference concern supports or services to NDIS participants
- applicants under the FOI Act, or Accredited Users and Accredited Data Service Providers who apply for access to NDIS Commission data under the *Data Availability and Transparency Act 2022*.

Data sharing and matching

The NDIS Commission may use information – including personal information – for data matching and analytics. This helps us regulate NDIS providers and workers so they deliver safe, good quality supports to NDIS Participants. For more information, see [Fraud](#).

The NDIS Commission may use personal information, for data matching, analytics and AI-supported processing. This includes identifying trends, patterns and risks to support NDIS Commission regulatory functions and activities such as improving service delivery by NDIS Providers.

9. Disclosure of personal information to overseas recipients

The NDIS Commission may disclose personal information about an individual to an overseas recipient in the course of performing our functions and activities. For example - in relation to a law enforcement matter (such as a criminal investigation), or third-party service providers (located overseas) who assist to conduct surveys, research or use cloud services with servers outside Australia.

Additionally, certain tools, such as Google Analytics and Google reCAPTCHA will store data overseas on Google's servers. [Read about how Google Analytics collects and stores data \(Opens in a new tab/window\) from our sites.](#)

Other countries we may disclose information to include the United States, Hong Kong, New Zealand, the United Kingdom and Singapore. We will not disclose personal information to an overseas recipient without express or implied consent, unless otherwise permitted by APP 8 Cross-border disclosure of personal information.

10. Quality, access, and correction

The NDIS Commission takes reasonable steps to ensure that the personal information we hold is accurate, up to date, relevant and complete, including at the time of using or disclosing the information and having regard to the purpose of the use or disclosure. This includes personal information used and contained in AI-generated and LLM-generated outputs.

Under the Privacy Act an individual is able to seek access to their personal information and request correction if the information is inaccurate, outdated, incomplete, irrelevant or misleading. Generally, an application under the Privacy Act for access will be acknowledged within 30 days from the date that we receive it.

In processing access requests, we may refuse access or correction of personal information where there are valid reasons to do so under the Privacy Act, the FOI Act or other applicable law – for example, where access is unlawful under a secrecy provision in portfolio legislation, or where the personal information held is an opinion and not an objective fact. We will provide reasons for our decision and set out how to request a review if you do not agree with our assessment.

To access or seek correction of personal information we hold about you, please contact us using the contact details set out at section 12 of this Privacy Policy.

It is also possible to access, and correct documents held by the NDIS Commission under the FOI Act. For information on this, please visit our FOI page.

11. Online interactions

Our website

When you visit the NDIS Commission website, a record of your visit is made which may include information about:

- your browser, domain name and operating system
- date and time of access and downloaded documents, and
- if you have accessed our website via a linked/referring webpage.

We use this information for statistical analysis and systems administration. We do not use the information to identify individuals or their browsing activities. However, some circumstances the NDIS Commission may need do so if required or authorised by law to disclose this information.

The NDIS Commission also uses Google Analytics which are web analysis services provided by Google Inc. ('Google'). All the information we collect using Google Analytics is for internal purposes and does not allow an individual to be identified.

The NDIS Commission uses antispam tools such as Google reCAPTCHA that distinguish a real user from bots. The tool may collect data about how you interact with the website and our forms, and that data may be stored on Google's servers outside of Australia. Content that you enter in the Commission's online forms will not be collected through this tool.

Google reCAPTCHA may collect data about how you interact with the NDIS Commission's smart forms, including:

- mouse movements
- device IP address
- date and time when pages were accessed
- device type, operating system and browser information
- device screen size, and
- geographic location (city).

Cookies

The NDIS Commission may use cookies to maintain contact with a user during a website session and to remember settings, preferences, or activity across multiple sessions. A cookie is a small file that is placed on your computer by your web browser.

Cookies allow the NDIS Commission's website to offer consistent experiences across multiple sessions, to recognise a returning browser, and to track usage patterns as users navigate the site.

This enables the NDIS Commission to collect aggregated information about how the website is used, such as the pages visited, the average time spent on each page, and the number of visitors.

Third party websites

Our website contains links to third party websites and social media platforms – for example, Facebook, LinkedIn and third-party survey providers. These websites may use web measurement tools, customisation technologies and persistent cookies to inform services.

The NDIS Commission do not use or share personal information made available through social media platforms including Facebook, LinkedIn and YouTube.

We are not responsible for the privacy practices or the content of websites maintained by third parties. Website functionality of third parties may capture and store your personal information outside Australia. Some third parties are not subject to the Privacy Act, and we encourage you to consult the privacy policies of other sites for information about their policies and practices.

Email addresses

The NDIS Commission records your email address if you send us an email or provide this on a form. It will only be used or disclosed in accordance with our obligations under the Privacy Act. We do not add email addresses to our automatic mailing list unless you request us to do so.

Electronic newsletters or subscriptions

To subscribe to our newsletter or other training services you must provide a valid email address. When we send you an electronic newsletter or you attend one of our education sessions, we have access to data about whether you opened that newsletter and attended an online event. These details will only be used or disclosed in accordance with our obligations under the Privacy Act and will not be added to any other mailing lists unless you specifically ask us to.

12. Feedback and complaints

How to contact the NDIS Commission

If you have feedback about our privacy practices or believe that the NDIS Commission has used your personal or sensitive information in a way that is not consistent with this Privacy Policy, the Privacy Act, the APPs or the Privacy Code, you can contact us by using the details set out at section 13 of this Privacy Policy.

We deal with complaints in accordance with our Feedback and Complaints Policy and we may seek further information in order to provide a full and complete response. We are committed to a fair and impartial resolution of any complaints without reprisal.

If you are not satisfied with our response, you may refer the complaint to the OAIC.

How to complain to the OAIC

You can contact the OAIC if you wish to make a privacy complaint against the NDIS Commission, or if you are not satisfied with how we have handled a complaint made to us in the first instance.

The OAIC website contains information on how to make a privacy complaint. If you make a complaint directly to the OAIC rather than to the NDIS Commission, the OAIC may recommend you try to resolve the complaint directly with the NDIS Commission in the first instance.

13. How to contact us

Request a copy of the Privacy Policy, submit a query or make a complaint

If you would like to:

- request a physical copy of the PDF version of our Privacy Policy,
- make a privacy complaint or have a query
- request information about how you can access or seek correction of your personal information

you can contact the NDIS Commission using the details below:

Email: privacy@ndiscommission.gov.au

Telephone: 1800 035 544 (request to be transferred to a Privacy Officer)

Post:

NDIS Commission – Privacy Team

PO Box 210

Penrith NSW 2750

Contact details for freedom of information (FOI) requests

Access to some information that we hold may require a formal request under the FOI Act. FOI applications and queries should be made to:

- **Email:** foi@ndiscommission.gov.au
- **Post:** NDIS CommissionFOI Team, PO Box 210, Penrith NSW 2750.

14. NDIS Commission Personnel

This Privacy Policy also applies to all NDIS Commission Personnel undertaking activities at the NDIS Commission. The NDIS Commission collects and handles personal information for the purposes of recruiting and employing Personnel. The types of personal and sensitive information we collect and hold about Personnel include:

- identification information (DOB, passport, drivers licence details etc)
- job applications, resumes and qualification documents

-
- contract details, referee and emergency contact details
 - employment contracts, contractor engagement and associated records
 - salary, leave, superannuation, taxation and banking details
 - clearances, medical certificates and health related information
 - information relating to conduct and performance

The NDIS Commission will generally collect personal information directly from Personnel. We may also collect information from other persons, such as supervisors, recruitment agents, and previous employers.

The NDIS Commission may collect and use your sensitive (i.e. health information) and personal information to maintain your health and safety and that of work colleagues. Sensitive and personal information may be disclosed to relevant NDIS Commission areas and/or a senior supervisor strictly on a need to know basis. The NDIS Commission be legally required, to disclose health and other personal information to other government entities, or third-party service providers including, but not limited to; health authorities for health and safety purposes.

More information about how the NDIS Commission manages personal information related to Personnel is accessible on the intranet Privacy page.

15. Key appointments and roles

Privacy Champion

The Director of the Privacy team is the Privacy Champion for the NDIS Commission, and is responsible for:

- promoting a culture of privacy within the NDIS Commission that values and protects personal information
- providing leadership within the NDIS Commission on broader strategic privacy issues
- reviewing and/or approving our privacy management plan and documented reviews of our progress against the plan, and
- providing regular reports to the executive, including about any privacy issues arising from our handling of personal information.

Privacy Officers

The Assistant Directors and Senior Review Officers of the team are the Privacy Officers for the NDIS Commission. This role is responsible for:

- handling of internal and external privacy enquiries, privacy complaints, and requests for access to and correction of personal information made under the Act
- maintaining a record of our personal information holdings
- assisting with the preparation of privacy impact assessments conducted under section 12 of the Privacy Code

-
- maintaining a register of privacy impact assessments as required by section 15 of the Privacy Code, and
 - measuring and documenting our performance against the privacy management plan at least annually as required by section 9 of the Privacy Code.

16. Personnel responsibilities

All Personnel have responsibilities under the Privacy Code and the Privacy Act to:

- undertake privacy education or training when provided by the NDIS Commission
- familiarise themselves with this Privacy Policy, and the APPs
- for Personnel in leadership positions, take positive steps to ensure that Personnel they supervise comply with their privacy-related responsibilities
- ensure personal information is lawfully collected and recorded, and only used or disclosed appropriately, in accordance with all legal obligations
- ensure personal information we hold is relevant, accurate and up to date, stored and archived in accordance with records management obligations and, if it is no longer relevant or necessary to be held that it is appropriately disposed of or de-identified, and
- ensure contracted service providers are contractually bound to comply with relevant law and policies, including the Privacy Act, the NDIS Act, and this Privacy Policy, through appropriate contractual provisions.

Accountability for AI-generated outputs

Personnel must be able to explain, justify and take ownership of any decision, action or outcome informed using AI tools, including LLMs.

This includes ensuring that:

- AI-generated or LLM-generated outputs are critically reviewed and validated prior to use
- decisions are not based solely on AI-generated or LLM-generated outputs
- appropriate records, markings and security classifications are applied to content that includes or is derived from AI-generated or LLM-generated information, and
- accountability for final decisions remains with authorised Personnel.

17. Further information

Privacy Impact Assessments

The NDIS Commission completes a privacy impact assessment (**PIA**) for all projects that might have a significant change to how we handle personal information, or a significant impact on the privacy of individuals. Our PIA Register can be accessed [here](#).

Privacy guidance

For further information about our privacy practices, contact either the Privacy Champion or Privacy Officers of the Assurance – Privacy Team at privacy@ndiscommission.gov.au

The Privacy Act is accessible at [*Privacy Act 1988 \(Cth\)*](#)

The Privacy Code is accessible at [*Privacy \(Australian Government Agencies - Governance\) APP Code 2017*](#)

Extensive guidance from the Office of the Australian Information Commissioner is available at [*Privacy*](#)

The NDIS Act is accessible at [*National Disability Insurance Scheme Act 2013 \(Cth\)*](#)