



**NDIS Quality
and Safeguards
Commission**

Privacy Policy



**NDIS Quality
and Safeguards
Commission**

NDIS Quality and Safeguards Commission PO Box 210, Penrith NSW 2750.

Copyright

© Commonwealth of Australia 2023



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 third party material
- any material protected by a trademark
- 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 2023

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

Contents

Contents	3
1. Purpose and Scope	4
2. What information we collect	4
3. How we collect information	5
4. Anonymity and pseudonymity.....	6
5. How we store and secure personal information	6
6. Responding to data breaches	7
7. Use and disclosure of personal information	7
8. Disclosure of personal information to overseas recipients.....	8
9. Access and correcting your personal information.....	8
10. Visiting our website and social media pages	9
11. Our website.....	9
12. Cookies.....	9
13. Electronic communication	10
14. How to complain to the NDIS Commission	10
15. How to complain to the OAIC.....	10
16. General enquiries and requests to access or correct personal information.....	10
17. Contact details for privacy complaints	11
18. Contact details for freedom of information requests	11
19. NDIS Commission Staff	11
20. Staff Responsibilities.....	12
21. Commission Information handled by the Department of Social Services.....	12
22. Further Information.....	12

1. Purpose and scope

The NDIS Quality and Safeguards Commission (**NDIS Commission**) is an independent agency established to improve the quality and safety of NDIS supports and services. The NDIS Commission's Privacy Policy sets out how the NDIS Commission will collect, hold and disclose personal and sensitive information in accordance with privacy laws.

The [Privacy Act 1988](#) (Cth) (**Privacy Act**) requires the NDIS Commission to handle personal information (including sensitive information) we collect about individuals in accordance with the Australian Privacy Principles (**APPs**) provided in Schedule 1 of the Privacy Act.

Under APP 1, the NDIS Commission is required to manage personal information in an open and transparent way.

In accordance with APP 1, our Privacy Policy outlines:

- the type of personal information we collect and hold
- how we collect and hold personal information
- the purpose for which we collect, hold, use and/or disclose personal information
- how an individual can access personal information about the person that is held by the NDIS Commission and seek correction of the information
- how an individual can make a complaint about our handling of personal information and how the NDIS Commission will deal with such a complaint;
- whether the NDIS Commission is likely to disclose personal information to overseas recipients, and if so, the countries in which those recipients are located.

In addition to the Privacy Act, the NDIS Commission and its officers must also comply with the secrecy provisions contained in the *National Disability Insurance Scheme Act 2013* (**NDIS Act**). These provisions limit how we record, disclose and use information about a person (including a deceased person) that is or was held in the records of the NDIS Commission.

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 about you when it is reasonably necessary for, or directly related to our functions or activities, or when required to do so by law.

We may collect sensitive information about you:

- where you consent
- when the collection is authorised or required by law
- when the collection is otherwise allowed under the Privacy Act

Examples of circumstances in which the NDIS Commission collects your information include:

- when you apply for registration as an NDIS provider
- when you make a complaint to us
- during compliance and enforcement activities or investigations
- requesting to be placed on a mailing list

-
- applying for a job at the NDIS Commission
 - when lodging a request for documents under the *Freedom of Information Act 1982* (Cth) (FOI Act).

Personal information is information or an opinion about an identified individual or an individual who is reasonably identifiable.

The personal information we may collect includes:

- contact details (such as your name, address, email and telephone numbers)
- biographical data (such as your date and place of birth, and gender)
- employment status and history (such as previous employment)
- education status
- financial information (such as bank details)
- government identifiers (such as Centrelink and Medicare Reference Numbers)
- information about your family and other related persons (such as any partners, children, dependants, carers or nominees or authorised representatives)
- information relating to feedback, complaints or applications made to us

Sensitive information is a subset of personal information that requires greater protection under the Privacy Act. Sensitive information includes information about:

- racial or ethnic origin
- political opinions or membership of a political association
- religious beliefs or affiliations
- philosophical beliefs
- membership of a professional or trade association or trade union
- sexual orientation
- criminal record
- health information
- genetic information
- biometric information or templates

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

We may also obtain photos and videos of you.

3. How we collect information

We collect personal information through various means including paper and electronic forms, online portals, written correspondence, face to face and over the phone discussions. If it is reasonable and practical to do so, we will collect personal information directly from the individual or their authorised representatives.

We may also collect personal information from third parties (e.g. NDIS providers, other government agencies and law enforcement agencies) in a variety of circumstances including, but not limited to:

- in the lodgement of a complaint
- in the context of compliance and enforcement activities
- in carrying out registration and other statutory functions
- recruiting our employees and contractors

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 may not inform you where:

- you have consented to the collection of your personal information from a third party
- we are required or authorised by law to collect the personal information from third parties, or
- it would not be reasonable or practicable to notify you that we have collected your personal information (for example, were notification could jeopardise an ongoing investigation)

4. Anonymity and pseudonymity

The Privacy Act requires us to provide individuals the option of not identifying themselves or using a pseudonym (made-up name) in their dealings with the NDIS Commission when it is lawful and practicable to do so – for example, where an individual wants to make an anonymous complaint.

When contacting the NDIS Commission, you should consider whether you want to remain anonymous or share your personal details. Generally, individuals can choose to remain anonymous or adopt a pseudonym 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. The NDIS Commission will inform you when this is the case.

5. 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, including laptop computers and mobile phones
- third party storage providers such as cloud storage facilities

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) (**Archives Act**) or any other applicable laws

5.1 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 that there has been such unauthorised access or disclosure, we will undertake an assessment to determine if it is an ‘eligible data breach’ within 72 hours and take all reasonable steps to contain the unauthorised access or disclosure. We will complete our assessment to determine if an eligible data breach has occurred within 30 days of becoming aware of the potential breach.

6. Use and disclosure of personal information

The NDIS Commission will only use or disclose personal information as set out in this policy and for the primary purpose for which it is collected. We may use or disclose personal information for another (secondary) purpose, if one of the following applies:

- the individual has consented to the use or disclosure
- the individual would reasonably expect us to use or disclose the personal information because it relates to the primary purpose for which it was collected (or if it is sensitive information, that it is directly related)
- we are required or authorised by law to use or disclose the information
- a permitted general situation exists—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, or for the compliance or enforcement activities of other Commonwealth, state or territory agencies

We may disclose your personal information to the following types of bodies or individuals:

- contracted service providers, lawyers and any other service providers who we engage to assist us with our functions

-
- other government agencies (such as the National Disability Insurance Agency (**NDIA**))
 - courts and tribunals
 - other law enforcement bodies (such as the Australian Federal Police)
 - 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)
 - responsible Ministers and parliamentary committees exercising their oversight functions
 - applicants under the FOI Act
 - referees and former employers to verify qualifications and experience when assessing certain applications
 - the Australian Government Security Vetting Agency or any other vetting providers that we engage to conduct security or vetting assessments on our behalf

6.1 Disclosure of personal information to overseas recipients

The NDIS Commission may disclose personal information about an individual to an overseas organisation in the course of providing our functions, for example to conduct a survey, research, or use a cloud service provider, which stores data outside Australia.

We will however take all reasonable steps not to disclose personal information to an overseas recipient unless:

- we have obtained your express or implied consent
- we are satisfied that the overseas recipient is compliant with the APPs, or equivalent regime
- we have formed the opinion that disclosure will lessen or prevent the health, safety or a serious threat to life of an individual or to public safety

Where applicable, we will comply with the Department of Home Affairs Hosting Certification Framework in respect to procuring offshore hosting arrangements.

7. Access and correcting your personal information

The NDIS Commission takes all reasonable steps to ensure that personal information we hold, use and disclose is accurate, complete and up-to-date, including at the time of using or disclosing the information.

You have a right under the Privacy Act to access and request corrections to personal information if you think the information is inaccurate, out-of-date, incomplete, irrelevant, or misleading. However, in some circumstances, the NDIS Commission may decline access to or correction of personal information – 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.

To access or seek correction of personal information we hold about you, please contact us using the contact details set out at section 10 of this 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](#).

8. Visiting our website and social media pages

The NDIS Commission website and social media pages may (at times) contain links to other third-party websites outside the NDIS Commission. The NDIS Commission is not responsible for information stored, accessed, used or disclosed on these third-party websites.

8.1 Our website

The NDIS Commission manages the majority of its website internally. If you visit our website to read or download information, we may record a range of technical information, which does not reveal your identity. This information includes your IP or server address, your general locality and the date and time of your visit to the website. Information is used for statistical and development purposes. No attempts are made to identify you through your browsing other than in exceptional circumstances, such as an investigation into the improper use of the website.

Website functionality of third parties may capture and store your personal information outside Australia. These third parties include, but not limited to:

- Facebook
- LinkedIn
- YouTube
- Campaign Monitor
- SurveyMonkey
- Google

These third parties may not be subject to the Privacy Act.

The NDIS Commission is not responsible for the privacy practices of third parties and encourages you to examine the privacy policies of these third parties and make your own decision regarding the reliability of material and information found.

8.2 Cookies

The NDIS Commission may use Cookies to maintain contact with a user through a website session. A cookie is a small file supplied by the NDIS Commission and stored by your web browser software on your computer when you access the NDIS Commission website.

Cookies allow the NDIS Commission to recognise an individual web user as they browse the NDIS Commission website. This allows the NDIS Commission to collect information about the way individuals use our website including, the pages viewed, average time spent on specific pages and the number of users visiting our website. No attempts are made to identify you through your browsing.

8.3 Electronic communication

There is an inherent risk associated with the transmission of information over the Internet, including via email. You should be aware of this when sending personal information to us by email or by using the NDIS Commission website.

If you are concerned about electronic communication, you may prefer to use other methods of communication with the NDIS Commission, such as post, fax or via phone.

9. Complaints

9.1 How to complain to the NDIS Commission

If you believe that the NDIS Commission has used your personal or sensitive information in a way that is not consistent with this policy or privacy laws, you can make a complaint by contacting us using the contact details set out at section 10 of this Policy.

We will respond to your complaint or request promptly in line 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 OAIC.

9.2 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.

10. How to contact us

10.1 General enquiries and requests to access or correct personal information

If you wish to:

- query how your personal information is collected, held, used or disclosed
- ask questions about this Privacy Policy
- obtain access to or seek correction of your personal information,

please contact the NDIS Commission using the following contact details:

- **email:** contactcentre@ndiscommission.gov.au
- **telephone:** 1800 035 544
- **post:** NDIS Commission Feedback, PO Box 210, Penrith NSW 2750.

10.2 Contact details for privacy complaints

If you wish to make a complaint about a breach of your privacy, please contact the NDIS Commission using the following contact details:

- **Email:** internalintegrity@ndiscommission.gov.au
- **Post:** NDIS Commission Internal Integrity, PO Box 210, Penrith NSW 2750.

10.3 Contact details for freedom of information 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 Commission Feedback, PO Box 210, Penrith NSW 2750.

11. NDIS Commission Staff

This policy applies to all NDIS Commission staff. ‘Staff’ means all persons employed or otherwise engaged by the NDIS Commission, and includes any volunteer or contractor to the NDIS Commission.

11.1 Key Appointments and Roles

Privacy Champion

The Director of the Internal Integrity Unit 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 Officer

The Assistant Director and Senior Review Officer of the Internal Integrity Unit 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.

11.2 Staff Responsibilities

All staff, in order to fulfil our responsibilities under the Privacy Code and the Privacy Act, must:

- undertake privacy education or training when provided by the NDIS Commission
- familiarise themselves with this Policy, and the Australian Privacy Principles at Appendix 4
- for staff in leadership positions, take positive steps to ensure that staff 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
- ensure personal information is stored and archived in accordance with records management obligations and, if it is no longer relevant or necessary to be held, ensure that it is appropriately disposed of or de-identified.
- ensure contracted service providers are contractually bound to comply with relevant law and policies, including the Privacy Act, the NDIS Act, and this Policy, through appropriate contractual provisions.

11.3 Information Protection obligations in the NDIS Act

In addition to being familiar with their obligations under the Privacy Act and specifically under the APPs, staff should also be aware of their responsibilities under Division 2 of Part 2 of Chapter 4 of the *National Disability Insurance Scheme Act 2013 (Cth)* (the NDIS Act). This Division deals with protected NDIS Commission information, as defined by section 9 of the NDIS Act, and sets out the general limitations on the use and disclosure of protected Commission information. Generally, all personal information held by the NDIS Commission falls within the broader definition of protected Commission information.

Sections 67B – 67D of the NDIS Act include criminal offence provisions relating to the unauthorised use or disclosure of protected Commission information and for soliciting disclosure or offering to supply protected Commission information.

The NDIS Commission may conduct audits to ensure that employees comply with these information protection obligations.

12. Commission Information handled by the Department of Social Services

The Department of Social Services (DSS) provides shared services to us, including human resources and information technology services. These mean that some of our personal information is stored on DSS systems. DSS are subject to the Privacy Act and manage information in accordance with their statutory obligations.

13. Further Information

For further information, contact either the Privacy Champion or Privacy Officers of the Internal Integrity Unit at internalintegrity@ndiscommission.gov.au.

The NDIS Commission easy read Privacy Policy is available at [Easy Read information | NDIS Quality and Safeguards Commission](#).

The Privacy Act is accessible at <https://www.legislation.gov.au/Details/C2019C00241>.

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

The NDIS Act is accessible at <https://www.legislation.gov.au/Details/C2019C00313>.