

Artificial Intelligence (AI) use

Version:2

Published:21 Jul 2026, 4:55 PM

Last edited:21 Jul 2026, 4:43 PM

Approved:21 Jul 2026, Ryan Wait

Next review:22 Feb 2027

Please note: This policy relates to rapidly evolving technologies. As such, we strongly recommend that you review and customise it to suit your specific organisational practices and standards.

Introduction

This policy provides guidelines for the appropriate use of artificial intelligence (AI) technologies within our organisation.

Determining whether the use of an AI technology is appropriate depends on:

- the specific tool being used
- the reasons for its use
- the applicable laws and standards governing its use.

As AI technologies continue to evolve, our organisation is dedicated to establishing a reliable system of practices that ensures flexibility for adaptation and effective use while prioritising privacy, safety, and compliance.

Applicability

When
• applies when using any tools or application that utilise AI technologies.
Who
• applies to all workers at every level of the organisation.

AI types and examples

AI encompasses a broad spectrum of tools and applications that serve many different purposes.

Refer to the table below for an overview of different AI tools.

This is not an exhaustive list and should be used only as a reference. The guidelines in this policy apply to all AI tools, even if they are not specifically referenced below.

AI Tool	How it is used	Examples
Natural Language Processing (NLP)	Text summarisation, translation, chatbots	ChatGPT, Google Translate, Grammarly, TextBlob

Computer Vision	Image recognition, accessibility aids	Google Cloud Vision AI, OpenCV, Microsoft Azure Computer Vision, Seeing AI
Machine Learning Platforms	Predictive analytics, anomaly detection	TensorFlow, Scikit-learn, AWS SageMaker, H2O.ai
Generative AI	Content creation, artistic design	DALL·E, MidJourney, Runway ML, Jukebox, Suno
Accessibility and Assistive	Text-to-speech, speech-to-text, mobility aids	Dragon NaturallySpeaking, Be My Eyes, Otter.ai, Voiceitt
Decision Support	Risk assessment, financial predictions	IBM Watson Health, RapidMiner, DataRobot, Power BI
Chatbots and Virtual Assistants	Customer support, scheduling, inquiries	ChatGPT, Amazon Alexa, Google Assistant

AI core use principles

All workers at every level of the organisation must adhere to the following core AI use principles:

- Maintain human decision-making at the core of all supports, services, and communications.
- Ensure AI enhances support delivery without compromising participant decision-making, privacy, preferences, safety, or outcomes.
- Be aware of which specific AI tools can and cannot be used within the organisation.
- Clearly communicate with participants and stakeholders when and how AI tools are used in supports and interactions.
- Unless otherwise specified, exclude all identifying information about anyone in the organisation (including participants, workers, or any stakeholders) when inputting information into AI tools.
- Maintain legal and regulatory compliance with
 - NDIS practice standards
 - [The Australian Privacy Principles \(APPs\)](#)
 - Relevant laws specific to our state/territory laws
- Manually review, quality check and modify all AI output as required, with consideration for output accuracy and relevance.
- Ensure relevant approved AI tools are accessible and do not create barriers for participants with diverse needs or abilities.
- Use AI tools responsibly to minimise biases and ensure equitable outcomes for all participants.
- Be transparent about AI usage and its impact on organisational operations and supports.
- Always be aware of risks associated with AI technologies, including but not limited to:
 - inaccurate information
 - lack of transparency around how AI tools store and manage data
 - discrimination and bias
 - data breaches and loss of control over personal information
 - misuse of tools to scam or deceive.
- Never use AI tools for deceptive practices or purposes that conflict with the NDIS code of conduct and the code of conduct of our organisation.

AI and personal data

When utilising AI technologies, our organisation will manage personal data in line with the guidance provided by the [Office of the Australian Information Commissioner \(OAIC\)](#).

In general, **information that is not freely and publicly available must never be inputted into any AI engines** without prior authorisation from key management personnel as this can lead to data breaches and misuse. This data includes, but is not limited to:

- organisational information that is not freely and publicly available (e.g. financial information, internal correspondence).
- any participant information
- any worker information.

Responsibilities of key management personnel

In addition to our core use principles, key management personnel are also responsible for:

- Encrypting all personal, sensitive, and identifying data.
- Managing the organised rollout of new AI tools in accordance with all relevant legal and compliance frameworks.
- Ensuring appropriate access control around:
 - what AI tools workers are allowed to use in a work context
 - who is allowed to use which specific tools
 - when and how a worker can use AI tools.
- Communicating the contents of this policy across the organisation.
- Conducting worker training around approved and safe use of AI.
- Maintaining awareness of the data use, storage and disposal policies of all AI tools that will be utilised within the organisation.
- Regularly evaluating AI tools and their usage to ensure alignment with the latest legal, ethical, and organisational standards.
- Maintaining awareness of the general terms of service for all AI tools that will be utilised within the organisation.
- Maintaining clear policies around data privacy, storage, handling, disposal, and use, which cover considerations related to AI.
- If intending to use any combination of AI and participant data, declaring this, and obtaining informed consent from all participants that are impacted.
- Ensure that all participants have accessible information around how our organisation uses AI technologies.

Responsibilities of workers

In addition to our core use principles, workers must:

- Only access AI tools that have been specifically approved for use by key management personnel.
- Use AI tools only in ways that have been approved by key management personnel.
- Participate in worker training around responsible and approved use of AI tools.
- Provide participants with accessible information around how AI tools are used within the organisation.
- If uncertain whether a specific use of AI is appropriate, escalate this question to relevant key management personnel as soon as practicable.

Examples of approved AI use

AI can be used for the following, provided full compliance with our core use principles and all other laws and guidelines.

- Improving participant accessibility in a way that aligns with the [NDIS framework for AI-enabled assistive technologies](#).
- Enhancing general worker training, for example through AI-powered training simulations.
- Analysing anonymised data to identify broad trends to improve service quality.
- General brainstorming, for example, producing a generic list of ideas for maintaining continuous improvement.
- Drafting general, non-sensitive documents such as progress report templates, provided these are manually reviewed and customised before they are used.

Workers at every level of the organisation must ensure that, even in approved use cases, AI complements and does NOT replace human experience, expertise and oversight.

Examples of prohibited AI use

The following are examples of AI use that are prohibited:

- Diagnosing health conditions.
- Making decisions or creating output (e.g., care plans, policies) without human review or intervention.
- Predicting participant behaviour, progress, or outcomes.
- Uploading/inputting any participant or organisational data into any AI tool without prior approval from key management personnel and participant consent.

Risk management

We will incorporate risks associated with AI use within our existing risk management system and proactively mitigate and manage these risks in line with relevant policies and processes.