



# Policy for the responsible use of AI in government

September 2024

Version 1.1

Digital Transformation Agency



© Commonwealth of Australia (Digital Transformation Agency) 2024 | Version 1801

With the exception of the Commonwealth Coat of Arms and where otherwise noted, this product is provided under a Creative Commons Attribution 4.0 International Licence. (<http://creativecommons.org/licenses/by/4.0/legalcode>)

The Digital Transformation Agency has tried to make the information in this product as accurate as possible. However, it does not guarantee that the information is totally accurate or complete. Therefore, you should not solely rely on this information when making a commercial decision.

Digital Transformation Agency is committed to providing web accessible content wherever possible.

If you are having difficulties with accessing this document, please email: [ai@dta.gov.au](mailto:ai@dta.gov.au).

Version: 1.1

# Contents

<b>Introduction</b> .....	<b>4</b>
<b>Policy aim</b> .....	<b>6</b>
Embrace the benefits.....	6
Strengthen public trust.....	6
Adapt over time.....	7
<b>Implementation</b> .....	<b>8</b>
Application.....	8
Existing frameworks.....	9
Artificial intelligence definition.....	9
<b>Principles and requirements</b> .....	<b>10</b>
enable and prepare.....	11
engage responsibly.....	13
evolve and integrate.....	14
<b>References</b> .....	<b>15</b>
<b>Attachment A - Related frameworks for AI</b> .....	<b>16</b>
<b>Attachment B - Risk assessment for use of AI</b> .....	<b>18</b>

# Introduction

The increasing adoption of artificial intelligence (AI) is reshaping the economy, society and government. While the technology is moving fast, the lasting impacts of AI on the activities of government are likely to be transformational.

This policy provides a framework to position the Australian Government as an exemplar under its broader safe and responsible AI agenda.

AI has an immense potential to improve social and economic wellbeing. Development and deployment of AI is accelerating. It already permeates institutions, infrastructure, products and services, with this transformation occurring across the economy and in government.

For government, the benefits of adopting AI include more efficient and accurate agency operations, better data analysis and evidence-based decisions, and improved service delivery for Australians. Many areas of the Australian Public Service (APS) already use AI to improve their work and engagement with the public.

To unlock innovative use of AI, Australia needs a modern and effective regulatory system. Internationally, governments have introduced new regulations to address AI's distinct risks, focused on preventative, risk-based guardrails that apply across the supply chain and throughout the AI lifecycle.

The Australian Government's consultations on safe and responsible AI show our current regulatory system is not fit to respond to AI's distinct risks.

They also found that **the public expects government to be an exemplar of safe and responsible adoption and use of AI technologies**. Public trust in AI and government's use of it is low, which acts as a handbrake on adoption. The preparedness and maturity for managing AI varies across the APS. AI technologies change at speed and scale, presenting further risks if not acted upon quickly.

Ultimately, this means government has an elevated level of responsibility for its use of AI and should be held to a higher standard of ethical behaviour.

The Australian Government's interim response to the consultations included a commitment to creating a regulatory environment that builds community trust and promotes innovation and adoption while balancing critical social and economic goals.

This policy is a first step in the journey to position government as an exemplar in its safe and responsible use of AI, in line with the Australian community's expectations. It sits alongside whole-of-economy measures such as mandatory guardrails and voluntary industry safety measures.

The policy aims to create a coordinated approach to government's use of AI and has been designed to complement and strengthen – not duplicate – existing frameworks in use by the APS.

In recognition of the speed and scale of change in this area, the policy is designed to evolve over time as the technology changes, leading practices develop and the broader regulatory environment matures.

## Policy aim

This policy aims to ensure that government plays a leadership role in embracing AI for the benefit of Australians while ensuring its safe, ethical and responsible use, in line with community expectations.

## Embrace the benefits

This policy provides a unified approach for government to engage with AI confidently, safely and responsibly, and realise its benefits.

The adoption of AI technology and capability varies across the APS. This policy is designed to unify government's approach by providing baseline requirements on governance, assurance and transparency of AI. This will remove barriers to government adoption by giving agencies confidence in their approach to AI and incentivising safe and responsible use for public benefit.

## Strengthen public trust

This policy aims to strengthen public trust in government's use of AI by providing enhanced transparency, governance and risk assurance.

One of the biggest challenges to the successful adoption of AI is a lack of public trust around government's adoption and use. Lack of public trust acts as a handbrake on adoption. The public is concerned about how their data is used, a lack of transparency and accountability in how AI is deployed and the way decision-making assisted by these technologies affects them.

This policy addresses these concerns by implementing mandatory and optional measures for agencies, such as monitoring and evaluation of performance, being more transparent about their AI use and adopting standardised governance.

## Adapt over time

This policy aims to embed a forward leaning, adaptive approach for government's use of AI that is designed to evolve and develop over time.

AI is a rapidly changing technology and the scale and nature of change is uncertain. This policy has been designed to ensure a flexible approach to the rapidly changing nature of AI and requires agencies to pivot and adapt to changes in the technological and policy environment.

# Implementation

## Application

This policy takes effect on **1 September 2024**.

Consistent with other whole-of-government digital policies, all Non-corporate Commonwealth entities (NCEs), as defined by the Public Governance, Performance and Accountability Act 2013, must apply this policy.

Corporate Commonwealth entities are also encouraged to apply this policy.

## National security carveouts

This policy does not apply to the use of AI in the defence portfolio.

This policy does not apply to the 'national intelligence community' (NIC) as defined by Section 4 of the Office of National Intelligence Act 2018.

The NIC includes:

- Office of National Intelligence (ONI)
- Australian Signals Directorate (ASD)
- Australian Security Intelligence Organisation (ASIO)
- Australian Secret Intelligence Service (ASIS)
- Australian Geospatial-Intelligence Organisation (AGO)
- Defence Intelligence Organisation (DIO)
- Australian Criminal Intelligence Commission (ACIC)
- the intelligence role and functions of the Australian Transaction Reports and Analysis Centre (AUSTRAC), Australian Federal Police (AFP), the Department of Home Affairs and the Department of Defence.

Defence and members of the NIC may voluntarily adopt elements of this policy where they are able to do so without compromising national security capabilities or interests.



## Existing frameworks

The challenges raised by government use of AI are complex and inherently linked with other issues, such as:

- the APS Code of Conduct
- data governance
- cyber security
- privacy
- ethics practices.

This policy has been designed to complement and strengthen – not duplicate – existing frameworks, legislation and practices that touch upon government’s use of AI.

This policy must be read and applied alongside existing frameworks and laws to ensure agencies meet all their obligations. While not exhaustive, a list of related frameworks is provided at **Attachment A**.

## Artificial intelligence definition

While there are various definitions of what constitutes AI, for the purposes of this policy agencies should apply the definition provided by the Organisation for Economic Co-operation and Development (OECD):

**I** An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment. **I**

Agencies may refer to further [explanatory material on the OECD website](#).

Given the rapidly changing nature of AI, agencies should keep up to date on changes to this definition. The definition in this policy will be reviewed as the broader, whole-of-economy regulatory environment matures to ensure an aligned approach.

# Principles and requirements

This section outlines the policy principles and requirements under the 'enable, engage and evolve' framework.

**enable | engage | evolve**





## enable and prepare

### Policy principles

- Safely engage with AI to enhance productivity, decision-making, policy outcomes and government service delivery for the benefit of Australians.
- APS officers need to be able to explain, justify and take ownership of advice and decisions when utilising AI.
- Have clear accountabilities for the adoption of AI and understand its use.
- Build AI capability for the long term.

### Mandatory requirements

#### Accountable officials

Agencies **must** designate accountability for implementing this policy to accountable official(s) within 90 days of this policy taking effect.

The responsibilities may be vested in an individual or in the chair of a body. The responsibilities may also be split across officials or existing roles (such as Chief Information Officer, Chief Technology Officer or Chief Data Officer) to suit agency preferences.

The responsibilities of the accountable officials are to:

- be accountable for implementation of this policy within their agencies
- notify the Digital Transformation Agency (DTA) where the agency has identified a new high-risk use case by emailing [ai@dta.gov.au](mailto:ai@dta.gov.au). This information will be used by the DTA to build visibility and inform the development of further risk mitigation approaches. Agencies may wish to use the risk matrix at **Attachment B** to determine risk ratings.
- be a contact point for whole-of-government AI coordination
- engage in whole-of-government AI forums and processes
- keep up to date with changing requirements as they evolve over time.

Agencies are to email the DTA when they designate and make any changes to their accountable official(s) by emailing [ai@dta.gov.au](mailto:ai@dta.gov.au).

## Recommended actions

### Staff training on AI

It is **strongly recommended** that agencies implement:

- AI fundamentals training for all staff, aligned to the approach under the policy guidance, within 6 months of this policy taking effect
- Additional training for staff in consideration of their roles and responsibilities, such as those responsible for the procurement, development, training and deployment of AI systems.

### Agencies should consider:

#### Understanding AI use

Understanding where and how AI is being used within agencies and developing an internal register with this information.

#### Existing frameworks

Integrating AI considerations into existing frameworks such as privacy, protective security, record keeping, cyber and data (see **Attachment A** for a more comprehensive list).



## engage responsibly

### Policy principles

- Australians are protected from harm.
- AI risk mitigation is proportionate and targeted.
- AI use is ethical, responsible, transparent and explainable to the public.

### Mandatory requirements

#### AI transparency statement

Agencies **must** make publicly available a statement outlining their approach to AI adoption and use within 6 months of this policy taking effect, as directed by the DTA.

The statement **must** be reviewed and updated annually or sooner, should the agency make significant changes to their approach to AI.

This statement must provide the public with relevant information about the agency's use of AI including information on:

- compliance with this policy
- measures to monitor effectiveness of deployed AI systems
- efforts to protect the public against negative impacts.

### Agencies should consider:

#### AI assurance framework pilot participation

Participating in the pilot of the Australian Government's AI assurance framework and providing feedback to the DTA on outcomes of the pilot to inform next steps.

Agencies interested in participating can seek more information by emailing: [ai@dta.gov.au](mailto:ai@dta.gov.au)

#### Applying the generative AI guidance

Applying the generative AI guidance.



## evolve and integrate

### Policy principles

- Flexibility and adaptability to accommodate technological advances.
- Ongoing review and evaluation of AI uses and the policy ecosystem.
- Feedback mechanisms embedded throughout government.

### Agencies should consider:

#### Monitoring and evaluation approaches

Reviewing on an ongoing basis the internal policies and governance approaches to AI to ensure they remain fit for purpose.

Monitoring AI use cases to assess for unintended impacts.

#### Integrating AI with a whole-of-government approach

Keeping up to date with changes in the policy and governance environment and pivot quickly to ensure ongoing compliance.

Engaging with whole-of-government capacity building to encourage APS-wide capability uplift over time.

# References

Department of Industry, Science and Resources (DISR) (2024) Safe and responsible AI in Australia consultation - Australian Government's interim response, DISR, Australian Government.

Department of the Prime Minister and Cabinet (PM&C) (2023) How might artificial intelligence affect the trustworthiness of public service delivery?, PM&C, Australian Government.

Office of the Australian Information Commissioner (OAIC) (2023) Australian Community Attitudes to Privacy Survey 2023, OAIC, Australian Government.

Productivity Commission (2023) 5-year Productivity Inquiry: Advancing Prosperity, Productivity Commission, Australian Government.

Bell G, Burgess J, Thomas J and Sadiq S. (2023) Rapid Response Information Report: Generative AI - language models (LLMs) and multimodal foundation models (MFMs), Australian Council of Learned Academies.

Organisation for Economic Cooperation and Development (OECD) (2019), Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449.

Russel S, Perset K and Grobelnik M (29 November 2023) 'Updates to the OECD's definition of an AI system explained', The AI Wonk - OECD.AI Policy Observatory

OECD (2024) Explanatory memorandum on the updated OECD definition of an AI system, OECD Artificial Intelligence Papers, No. 8, OECD Publishing, Paris.

# Attachment A

## Related frameworks for AI

While this section lists frameworks that are related to AI, it is not exhaustive. Agencies should consider what existing frameworks apply to them and their specific AI use cases.

### APS conduct

[APS Code of Conduct](#)

[Public Service Act 1999](#)

### Artificial intelligence

[Australia's AI Ethics Principles](#)

[Engaging with Artificial Intelligence \(AI\) guidance](#)

[Interim guidance on government use of public generative AI tools \(Generative AI guidance\)](#)

### Automated decision-making

[Automated Decision-making, Better Practice Guide](#)

[Australian Administrative Law Policy Guide](#)

Attorney-General's Department legislative framework for automated decision-making across the Australian Government (under development)

### Cyber and protective security

[2023-2030 Australian Cyber Security Strategy](#)

[Protective Security Policy Framework](#)

[Cyber Security Guidelines](#)



## Data

[Framework for Governance Indigenous Data](#)

[Foundational Four](#)

[Archives Act 1983](#)

[Data-matching Act 1990](#)

[Data Availability and Transparency Act 2022](#)

[Notifiable Data Breaches scheme](#)

## Digital investment

[Investment Oversight Framework](#)

[Data and Digital Government Strategy](#)

## Privacy

[Privacy Act 1988](#)

## Procurement

[Commonwealth Procurement Rules](#) and procurement policies

[Digital Sourcing Contract Limits and Reviews Policy](#)

## Risk

[Commonwealth Risk Management Policy](#)

## Intellectual property

[Copyright Act 1968](#)

[Intellectual property principles for Commonwealth entities](#)

# Attachment B

## Risk assessment for use of AI

		Consequence				
		Insignificant	Minor	Moderate	Major	Severe
Likelihood	Almost certain	Medium	Medium	High	High	High
	Likely	Medium	Medium	Medium	High	High
	Possible	Low	Medium	Medium	High	High
	Unlikely	Low	Low	Medium	Medium	High
	Rare	Low	Low	Low	Medium	Medium

**Figure 1:** Risk matrix for use of AI

Using the risk matrix, determine the severity of the risks. In considering the consequence and likelihood consult with relevant stakeholders. The risk assessment should reflect the intended scope, function and risk controls of the AI use case.

The policy does not prescribe risks that agencies should be assessing or the system used to determine the final risk outcomes.

The following are examples of risks that an agency can consider as part of their assessment.

What is the risk that the use of AI:

- negatively affects public accessibility or inclusivity of government services
- unfairly discriminates against individuals or communities
- perpetuates stereotypes or demeaning representations of individuals or communities
- causes harm to individuals, communities, businesses or the environment
- results in privacy concerns due to the sensitivity of the data being manipulated, parsed or transformed by the system
- results in security concerns due to the sensitivity or classification of the data being manipulated, parsed or transformed by the system

- results in security concerns due to the implementation, sourcing or characteristics of the system
- influences decision-making that affects individuals, communities, businesses or the environment
- poses a reputational risk or undermines public confidence in government
- results in intellectual property concerns due to the system manipulating, transforming or reproducing material for which a third party owns copyright.

Agencies should refer to existing risk management frameworks, such as the Commonwealth Risk Management Policy and internal agency risk management approaches, for guidance in assessing the concepts under the risk matrix at

**Attachment B.**