ACT Government

ACT Government Artificial Intelligence Policy

Version 1.0.

May 2025

We acknowledge the Ngunnawal people as traditional custodians of the ACT and recognise any other people or families with connection to the lands of the ACT and region. We acknowledge and respect their continuing culture and the contribution they make to the life of this city and this region.

Introduction

Purpose

This policy ensures the safe, ethical, and responsible use of artificial intelligence (AI) within the ACT Government. It provides a framework to guide the ACT Government to identify and manage benefits and risks associated with AI technologies, supporting innovative service delivery and decision-making that align with community expectations.

The ACT Government AI Policy and the ACT AI Assurance Framework align with Australia's AI Ethics Principles and National AI Assurance Framework, ensuring we meet key national standards and commit to maintaining community trust by developing AI solutions that are well-designed, safe, and appropriately governed.

There are a range of issues which may arise in the implementation and use of AI tools that are not covered by this policy. This policy is designed to address specific risks associated with these emerging technologies. It is not designed to be the sole lens through which any project that includes AI technology is understood or assessed. The comprehensive risk assessment associated with the Assurance Framework will continue to evolve to capture current and future risks associated with AI technologies.

The ACT Government will continue to undertake relevant considerations from a budgetary, human rights and workforce perspective, among other considerations.

The primary objective of this policy and framework is to establish the necessary guardrails specific to the use of AI.

Background

The CSIRO Artificial Intelligence Roadmap (2019) highlights AI applications across Australia, particularly within government sectors. The recommendations emphasise the importance of specialising in, investing in, and using AI technologies.

For government, AI presents opportunities to:

- enhance policy and service design and delivery
- streamline regulatory and compliance functions
- improve operational management of organisational digital and data assets
- address complex, multidisciplinary challenges
- deploy new capabilities.

AI adoption may introduce risks such as bias, privacy, security, governance and accountability. These could undermine the community's trust and willingness to engage with ACT Government services. As the technology evolves rapidly and ACT Government advances to more mature and complex uses of AI, we must develop appropriate governance processes to support initiatives and meet the needs and expectations of our community.

Scope

The policy and framework apply to AI initiatives where any of the following conditions are met:

- Use generative AI capabilities, even if these capabilities are part of standard commercially available products and are not modified.
- Use AI solutions specifically developed or trained for the ACT Government, internally or by external vendors (excludes configuration[1]).
- Use AI in commercially available products in new and novel ways. For example, creating a tailored solution specifically for the ACT Government. Standard usage of AI functionalities in commercially available solutions are exempt from this policy.[2]

Additional policy and legislative considerations

ACT Public Service (ACTPS) staff use of AI tools, such as generative AI technologies, is also covered by complementary policies and guidance including:

- Artificial Intelligence: When to use it and when to avoid it at work.
- the ACTPS Code of Conduct and all relevant human resources policies
- software usage regulations (for example, those governing Microsoft Outlook or the use of smart devices)
- all relevant legislation (notably the *Information Privacy Act 2014* outlined in Table 4).

What is AI?

AI is the capability of a computer system to use data and algorithms to perform tasks that normally require human expertise. These tasks currently include, but are not limited to:

- reasoning and planning
- natural language processing
- computer vision
- audio processing
- interaction
- identifying meaningful patterns
- decision-making
- prediction
- generating text, images, audio, and video.

[1] Excluding configuration means that the policy does not apply to basic setup or customisation of AI products that are already commercially available.

[2] Standard use AI functionalities as they are intended and provided by the vendor, without any modifications or special customisations, are exempt from the policy because they are routine and do not involve new or novel applications. For example, using a built-in AI feature in a software application for its intended purpose, like automated email sorting in an email client, would be considered standard use.

AI can be designed and used to operate with varying levels of automation. These technologies include, but are not limited to:

- **Machine learning**, enabling computer systems to learn from data.
- **Computer vision**, allowing computer systems to interpret visual information.
- **Natural language processing**, assisting in understanding and generating human language.
- **Generative AI**, producing audio, visual, text or code content with minimal intervention.

Key terms

- **AI technology** – An encompassing term that refers to the algorithms, tools, and techniques used to create or train AI models and the AI systems.
- **AI model** – A program that employs AI algorithms and techniques to solve complex tasks.
- **AI system** – A group of interacting elements including at least one AI model. In the case of generative AI, the system includes, but is not limited to, the large language model and the corpus of knowledge used by the model to generate an output.
- **AI initiative** – Any project or program that uses AI technology to achieve a specific outcome or improvement of operations.

Roles and responsibilities

Responsible officers

Directorates must identify four 'responsible officers' with specific roles and responsibilities for comprehensive oversight and management of AI initiatives.

Each role is independent and should be assigned to a different person.[3] Responsible officers should be senior, skilled, and qualified.

Responsible officer roles and responsibilities are similar to those in the Cyber Security Policy but have been tailored to the requirements of this policy. Shared responsibilities with roles in the cyber policy are not duplicated – meeting the requirements of one role automatically satisfies the other.

Table 1 lists each responsible officer's responsibilities and any overlaps in responsibilities with the cyber policy.

[3] For small-scale projects where this isn't feasible, risks arising from an individual occupying more than one 'responsible officer' role should be identified in the assurance assessment with strategies and actions to mitigate the risk.

Table 1. The responsibilities of each responsible officer.

Responsible officer	Responsibilities
AI system owner (overlaps with 'business system owner')	Person at executive or senior level within an administrative unit with the authority to: • oversee AI system insights and decisions • define the strategy • align goals and deliverables • ensure compliance with framework requirements • take responsibility for the initiative's outcomes.
AI system administrator (overlaps with 'system administrator')	An ACTPS officer with access privileges, knowledge, and skills necessary to manage and monitor the AI system's technical performance and deploy updates and changes.
Data custodian/steward	An ACTPS officer responsible for the data used in an AI system and meeting data governance and management requirements.
Project manager	An ACTPS officer who manages the AI system project scope, goals, and deliverables.

To comply with the policy, directorates must provide bi-annual summaries of their AI initiatives to the ACT AI Advisory Group for inclusion in an AI register. An abridged version of the AI register may be made public.[4]

At a minimum, these summaries must include:

- a brief description of the initiative and how AI is used
- key ethical considerations taken in designing the initiative
- a contact point (preferably a team or office's group email address or phone number).

The AI Advisory Group secretariat will manage details of this reporting arrangement. This includes requesting and collecting information, and administration of the public facing register.

Directorates should also nominate and document their initiative's responsible officers, in line with record keeping requirements.

To better integrate these roles, directorates can include their responsibilities or titles in relevant position descriptions. Additionally, they can develop directorate-specific policies outlining any additional responsibilities related to AI initiatives.

[4] A project is exempt from this reporting requirement if disclosing the nature of an AI-system is deemed inappropriate from a public safety perspective. For example, if a cyber security solution uses an AI component, knowledge of that fact could help a malicious threat actor.

Other relevant roles

There are other relevant roles essential for aligning, securing, and implementing AI technologies across the ACT Government. They focus on overarching strategies and coordination, providing leadership, governance, and technical oversight.

These roles work collaboratively with the responsible officers outlined in the policy to integrate AI solutions into our operations while maintaining compliance and security standards. Table 2 describes each role.

Table 2. The responsibilities of the other relevant roles.

Role	Responsibilities
ACT Chief Digital Officer (CDO)	• Develop and drive strategic digital solutions and strategies to enhance service delivery. • Set the vision and strategy for AI adoption and governance by ensuring alignment with digital strategy.
Chief Information Security Officer (CISO)	• Provide cyber security advice to initiative proposals as part of the AI Advisory Group, as required.
Chief information officers (CIOs) or Head of corporate	• Promote the responsible adoption of AI technologies within their directorates. • Oversee the use of AI tools within their directorates. This includes relevant cyber security mitigations, and any ethical considerations and required actions. • Maintain a register of all AI tools used in their directorates (as part of their reporting commitment to the AI Advisory Group). • Work with other roles in their directorates, such as legal, contracts, and HR, to address ethical, workforce and other considerations in the deployment of AI solutions.
Security and Emergency Management Division (SEMD) responsible officer	• Provide protective security advice to effectively manage the security of people, information, and assets.
Digital, Data and Technology Solutions (DDTS)	• Develop and implement ACT digital strategy, cyber security, and ICT policies. • Create and implement technology solutions, drive the use of data, oversee ICT investments, and provide ICT infrastructure and services.
Directors-general and agency heads	• Set the strategic direction for their directorate in line with government objectives. • Support and provide resources for AI initiatives as required. • Take full responsibility for the safe and responsible deployment of AI in their directorates.
ICT project managers (DDTS)	• Support ICT projects and operations, including AI technologies, and liaising between DDTS and directorate-based staff. Note: not all initiatives involve DDTS or ICT project managers.

ACT AI Advisory Group

The ACT Government has established the ACT AI Advisory Group (AIAG) to support the ethical, safe and effective development and rollout of AI in line with this policy and framework.

The AIAG provides advice and oversight for AI initiatives across the ACT Government and works in conjunction with existing ICT review and governance processes.

The AIAG has the following roles and responsibilities:

- Assess all 'in scope' AI initiatives and ensure they meet ethical and other requirements in line with the national AI assurance commitments, and ACT-specific human rights, wellbeing, environmental and workforce considerations as defined in this policy and framework.
- Advise AI system owners and project managers on the ethical feasibility of certain AI initiatives, offering guidance to reduce and mitigate risks.
- Suggest revisions to AI initiative proposals to meet policy standards.
- Provide input into the strategic direction of AI capability across the service, and on the usage and rollout of AI capability and tools.
- Support the design and delivery of AI risk assessment tools to all AI initiatives in scope of the policy.
- Report on the use of AI across the ACT Government.

Table 3 describes the composition of the AIAG, detailed in the AIAG terms of reference. The group's membership is subject to change as agreed by members and the Chair.

To support a consistent, whole-of-government approach, directorates must incorporate the AIAG as a function into their AI-related directorate governance processes. They are also encouraged to establish directorate-specific governance processes for AI initiatives before submitting them to the AIAG.

Table 3. The members and respective responsibilities of the AIAG.

Member	Responsibilities
Chair and deputy chair	• Chair: Executive Group Manager, DDTS. ○ An executive group manager appointed by the Data Reform Group (DRG) for 12 months and reviewed annually. • Deputy chair: An executive branch manager or executive group manager appointed by the Data Reform Group Chair for 12 months and reviewed annually.
Standing ex officio members	• Executive Branch Manager, Data, Artificial Intelligence and Digital Records Branch (DAIDR), DDTS, CMTEDD. • Executive Branch Manager, Access Canberra.
Directorate representatives	• Each directorate is represented by an executive branch manager, nominated by their DRG representative for 24 months. Meeting proxies are allowed, when necessary, with Secretariat approval. • Members may oversee their directorate's rollout of AI. They represent their directorate and conduct all required internal consultation, and briefing processes to the relevant DDG/DG through established directorate-specific channels. They provide insights and recommendations on behalf of their directorates, including conducting directorate-level consultation on proposals, as applicable.
AI subject matter experts	• Up to four subject matter experts. They are nominated by directorates and appointed by the chair and deputy chair, on advice from the Executive Branch Manager, DAIDR.
Additional specialist members	• To ensure a comprehensive focus on human rights, wellbeing, legislation, legal, safety and policy aspects, additional members will be included as ex-officio members who may send proxies when necessary.
Secretariat	• Lead rollout of AI capability across the ACT Public Service. • Drive the strategic agenda of the AIAG, in partnership with the chair and deputy chair, and under mandate from DRG. • Manage end-to-end secretariat support for the group. • Performed by DDTS (DAIDR).
Guests and presenters	• Presenters, guests, and observers may be invited to attend certain meetings, sponsored by a member, and approved by the chair. They will not become standing AIAG members.

Relevant legislation, policies, and other documents

Table 4. Other relevant documents to consider.

Legislation and policy	Description
National AI Assurance Framework	The National AI Assurance Framework establishes a joint approach, based on Australia's AI Ethics Principles, to safe and responsible AI. The national framework was agreed by Australian Data and Digital Ministers on 21 June 2024.
Human Rights Act	The ACT *Human Rights Act 2004* protects and promotes human rights. AI system owners, especially those in criminal justice, education, and detention contexts, should consider whether the AI system may infringe on an individual's rights.
Information Privacy Act	The *Information Privacy Act 2014* sets out the Territory Privacy Principles (TPPs), which govern how the ACT Government collects and uses data. This is important to AI systems trained on data.
Public Sector Management Act	The ACT *Public Sector Management Act 1994* regulates the administration of the public sector in the Territory including establishing the standards for public service jobs, public sector values and principles. It also provides the mechanism for handling changes in structures and positions.
ACT Wellbeing Framework	The ACT Wellbeing Framework informs our implementation of the National AI Ethics Principles by establishing an understanding of what impacts quality of life. Alignment ensures advancements in AI and community wellbeing are ethical, reliable, and centred on improving quality of life for all Canberrans.
Data Governance and Management Framework and other standards	The Data Governance and Management Framework (DGMF) supports the ACT Government develop its data maturity to deliver better outcomes for the community.
Cyber Security Policy	The ACT Cyber Security Policy is essential for protecting data used by all ACT Government ICT systems, including AI systems. It establishes security standards for the secure and ethical deployment of AI technologies, ensures compliance with government data protection obligations, maintains public trust, and aligns with the ACT Protective Security Policy Framework.

Legislation and policy	Description
Protective Security Framework	The ACT Protective Security Framework helps ACT Government entities protect their people, information, and assets by setting out government protective security policy and supporting entities to effectively implement the policy across security governance, information security, personnel security, and physical security.
Data Sharing Policy	Relevant to AI systems that use data from other agencies. The Data Sharing Policy defines the requirements for data sharing agreements within the ACT Government and with external entities. It ensures that data used in AI systems is deployed in a manner that is safe, legal, and trusted by the community.
ACT Digital Strategy	The ACT Digital Strategy sets out how the ACT Government will design AI services with the community in mind, leveraging technology to improve our quality of life and making Canberra a more liveable, sustainable, and connected city.

AI initiatives must comply with all relevant legislation.

AI ethics principles

The policy and framework align with Australia's AI Ethics Principles, guiding the ACT Government's use of AI to meet national standards and community expectations for ethical AI use. Table 5 describes each principle.

Table 5. National AI Ethics Principles.

Principle	Statement
1. Human, societal and environmental wellbeing	Throughout its lifecycle, each AI system should benefit individuals, society and the environment.
2. Human-centred values	AI systems should respect human rights, diversity and the autonomy of individuals.
3. Fairness	AI systems should be inclusive and accessible and should not involve or result in unfair discrimination against individuals, communities or groups.
4. Privacy protection and security	AI systems should respect and uphold privacy rights of individuals and ensure the protection of data.
5. Reliability and safety	Throughout their lifecycle, AI systems should reliably operate in accordance with their intended purpose.
6. Transparency and explainability	There should be transparency and responsible disclosure so people can understand when they are being significantly impacted by AI and can find out when an AI system is engaging with them.
7. Contestability	When an AI system significantly impacts a person, community, group or environment, there should be a timely process to allow people to challenge the use or outcomes of the AI system.
8. Accountability	Those responsible for the different phases of the AI system lifecycle should be identifiable and accountable for the outcomes of the AI systems, and human oversight of AI systems should be enabled.

ACT Public Service staff requirements

Under the policy and framework, staff must ensure that they:

- develop and use AI initiatives in alignment with directorate strategic plans, and broader ACT Government priorities
- demonstrate community or government advantages, such as improved service delivery or enhanced decision-making capabilities
- comply with all relevant privacy, security, and data protection laws
- implement strategies to minimise potential biases and risks in AI algorithms
- ensure that decisions made by the AI system are subject to human review and intervention.

AI Assurance Framework

This policy establishes the ACT AI Assurance Framework. The framework governs all AI initiatives in scope of this policy. Directorates must manage AI risk through use of the assurance self-assessment tool.

Completed self-assessments must be submitted to the AIAG for contestability review. Approval to proceed through the regular DDTS or directorate-specific project lifecycle governance will be granted, or recommendations on project risk management will be issued by the AIAG, based on this review.

All AI initiatives must be assessed against the framework at every stage, from the initial planning to the final delivery. Regular reviews should also be conducted to review established AI solutions.