HIGH COURT OF AUSTRALIA

A Guide to the Use of Artificial Intelligence (AI)

Distribution: All High Court of Australia employees, contractors and consultants.

CM Reference:

Summary: This policy has been developed to assist HCA staff in relation to the use of Artificial Intelligence (AI).

Document governance

Version number	Date of issue	Responsible Area	Description of change	Review by date
1	20/02/2026	ICT	Creation of policy	(1 year from date of issue)

Review Cycle

A review of the Artificial Intelligence (AI) Policy is taken every 1 year or following any significant changes to the High Court of Australia's broader environment.

Approval

Version number	Name	Position	Signature	Date
1	Richard Glenn	Chief Executive and Principal Registrar		20/02/2026

Contents

1. Introduction

This policy has been developed to assist High Court of Australia (HCA) Justices and staff in relation to the use of Artificial Intelligence (AI).

The aim of this policy is to foster a secure AI environment ensuring the integrity, confidentiality, and availability of the Court's systems, while embracing the innovation opportunities that Generative AI brings to the technological environment.

It sets out key risks and issues associated with using AI and some suggestions for minimising them. Examples of potential uses are also included.

Any use of AI by or on behalf of the Court must be consistent with the Court's overarching obligation to protect the integrity of the administration of justice.

This policy applies to all Justices, Chambers staff and HCA administration staff.

2. Common Terms

Algorithm:	A set of instructions used to perform tasks, such as calculations and data analysis, usually using a computer or another smart device.
Artificial Intelligence (AI):	Computer systems able to perform tasks normally requiring human intelligence.
AI Agent:	A software programme that uses AI to become aware of its environment, process information, and take actions to achieve its goals, based on the inputted information.
AI Prompt:	An input or instruction given to an AI system which will generate a specific response or result. Typically, a prompt is in the form of text, but many chatbots will now accept voice prompts.
Generative AI:	A form of AI which generates new content, which can include text, images, sounds and computer code. Some generative AI tools are designed to take actions.
Generative AI Tools:	A computer program which simulates an online human conversation using generative AI. Publicly available examples are ChatGPT, Google Bard and Meta AI.

Hallucination:	AI hallucinations are incorrect or misleading results that AI models generate. These errors can be caused by a variety of factors, including insufficient training data, the model's statistical nature, incorrect assumptions made by the model, or biases in the data used to train the model.
Large Language Model (LLM):	LLMs are AI models which learn to predict the next best word or part of a word in a sentence having been trained on enormous quantities of text. ChatGPT and Bing Chat use the OpenAI Large Language Model.
Machine Learning (ML):	A branch of AI that uses data and algorithms to imitate the way that humans learn, gradually improving accuracy. Through the use of statistical methods, algorithms are trained to make classifications or predictions, and to uncover key insights in data mining projects.
Natural Language Processing:	Programming computer systems to understand and generate human speech and text. Algorithms look for linguistic patterns in how sentences and paragraphs are constructed and how words, context and structure work together to create meaning. Applications include speech-to-text converters, online tools that summarise text, chatbots, speech recognition and translations.
Responsible AI:	The practice of designing, developing, and deploying AI with certain values, such as being trustworthy, ethical, transparent, explainable, fair, robust and upholding privacy rights.
HCA Issued Device	Electronic devices, such as smartphones, tablets, or laptops that are provided by the Court for work-related purposes.

3. Understanding different AI tools

3.1 Integrated AI

Common search engines such as Google and platforms such as Meta have integrated AI to enhance user experience and advertising. This is often displayed in search results as an 'AI overview'.

3.2 Public Generative AI tools

Public Generative AI Tools include products such as ChatGPT, Gemini, Firefly, Bard, Claude and others.

Public AI Tools do not provide answers from authoritative databases. They generate new text using an algorithm based on the prompts they receive and the data they have been trained upon. This means the output Public AI Tools generate is what the model predicts to be the most likely combination of words (based on the documents and data that it holds as source information). It is not necessarily the most accurate answer.

The current publicly available AI tools remember every question that you ask them, as well as any other information you put into them. That information is then available to be used to respond to queries from other users. As a result, anything you type into it could become publicly known.

3.3 Internal Generative AI

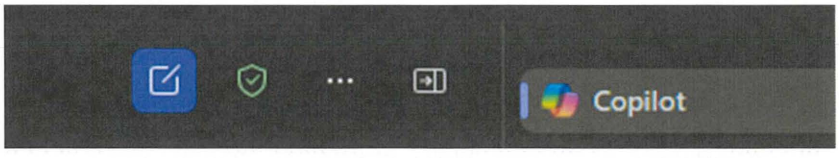
Distinct from Public generative AI tools, internal generative AI, has access to the Court's information and data as well as the internet.

Correctly configured, Internal generative AI tools provide greater assurance of the security and confidentiality of any information that is uploaded to them.

The only internal generative AI tool that meets the Court's security and confidentiality requirements is Microsoft 365 Copilot.

Copilot can be accessed via the Edge browser or the Microsoft 365 Copilot application. This tool provides enterprise data protection and operates within the privacy and security frameworks of Microsoft 365. When signed into your High Court account, the data you submit into Copilot is secure and will not be made public.

You must be logged into High Court network to ensure that any data you enter into Copilot is secure. You can confirm your session is secure by checking for the green shield icon in the top right corner of your screen, as shown below:



4. Core Principles

4.1 Acceptable AI tools

Microsoft 365 Copilot may be used on HCA issued devices when logged into the High Court network.

HCA devices may be used to access search engines with integrated AI capabilities, but consistent with existing security requirements, users must not enter any information that is sensitive, confidential, classified, personally identifiable, or otherwise not publicly available.

Public generative AI tools such as ChatGPT, Gemini, Firefly, Bard, Claude and others must not be used to enter any information that is sensitive, confidential, classified, personally identifiable, or otherwise not publicly available. These tools are blocked on HCA desktop and laptop computers but are accessible on HCA issued iPads and smartphones.

4.2 Take responsibility

Justices and High Court staff are responsible for material produced in their name, regardless of whether an AI tool is used to generate or assist in the creation of the material.

4.3 Verification

All AI-generated content must be verified against authoritative sources. AI outputs must never be relied upon without manual review. Justices and staff using AI must be alert to the possibility of "hallucinations"—plausible but false information generated by AI tools.

4.4 Maintain security

Follow best practices for maintaining your own and the Court's security.

Use work devices (rather than personal devices) to access Internal Generative AI tools.

5. Permitted Uses of AI

Justices and staff may use AI tools for the following purposes, subject to verification and oversight:

- Summarising lengthy documents or materials
- Undertaking preliminary legal research
- Drafting routine administrative correspondence
- Transcribing non-sensitive meetings or hearings
- Prioritising communications or managing workflow
- Assisting with document management and keyword search in large documents or datasets
- Creating timelines of relevant events
- Editing, proofreading or checking spelling and grammar

- Scheduling and calendar management
- Analysing operational data, administrative workflows and identifying efficiency improvements
- Enhancing the accessibility of court services
- Other uses as approved

6. Prohibited Uses of AI

AI must not be used for:

- Drafting the substantive reasoning of judgments
- Any task that substitutes for judicial discretion or independent analysis

7. Risks and Mitigations

7.1 Hallucinations

AI tools may:

- make up fictitious cases, citations or quotes, or refer to legislation, articles or legal texts that do not exist,
- provide incorrect or misleading information regarding the law or how it might apply, and
- make factual errors.

The accuracy of any information you have been provided by an AI tool must be checked before it is used or relied upon. It is critical that there is always a "human in the loop" when an AI tool is used.

7.2 Bias

AI tools based on LLMs generate responses based on the dataset they are trained upon. Information generated by AI will inevitably reflect errors and biases in its training data. Be alert to skewed perspectives.

7.3 Deepfakes and Manipulated Evidence

Remain vigilant for AI-generated or altered content. Consider forensic authentication where necessary.

7.4 "White Text" and Hidden Prompts

Documents may contain invisible prompts designed to manipulate AI tools. Always engage directly with the underlying source document.

8. Training and Review

Justices and staff are encouraged to undertake AI literacy training. This guide will be reviewed annually to reflect technological developments and evolving best practice.

9. Governance

Generative AI tools are rapidly evolving in their ability to support a variety of workplace tasks. When applied to the activities described in Part 5 of this Guide the use of AI is generally low risk.

However, any other proposed use that has implications for data integrity, sensitive data handling, system reliability, or decision-making transparency must undergo a structured approval process before implementation. This ensures that risks are appropriately assessed and managed, and that the Court maintains trust, security, and operational integrity.

Additionally, use cases should be subject to efficiency benchmarking to help evaluate their impact. This includes comparing productivity, accuracy, or time savings against traditional methods to ensure the adoption of Generative AI delivers a measurable value.

The approval process is outlined as follows:

1) Define the Exploratory use

Before initiating any exploratory use of Generative AI, staff must clearly describe the intended purpose and scope of the activity. This includes outlining the capability being trialled, identifying which systems, tasks, or processes may be impacted, and specifying the type of data involved. Any concerns relating to privacy, sensitivity, or compliance must be addressed as part of this definition.

2) Evaluation Method

A clear evaluation approach must be established to assess the effectiveness and appropriateness of the exploratory use. This should include defined success criteria, identification of potential risks, and a plan for mitigating those risks. Staff must also ensure that the setup, outcomes, and lessons learned are documented in a way that supports transparency and informs future decisions.

3) Approval and Oversight

No exploratory use of Generative AI other than those described in Part 5 may proceed without formal approval. The level of approval required will depend on the scope, impact, and strategic significance of the proposal. Reviews may be conducted by one or more of the following:

Chief Information Officer (CIO) – to evaluate technical feasibility and ensure appropriate information security controls are in place.

CE&PR – to confirm consistency with the organisation's strategic direction and acceptable risk thresholds.

Chief Justice – To provide endorsement for high impact or strategically significant proposals.

This oversight ensures that any proposals are considered with appropriate governance and safeguards in place.