Artificial Intelligence (AI)

Usage Policy

Version: 1.6

Last Updated: 16 June 2026

Effective Date: 16 June 2026

Table of Contents

Purpose

The purpose of this policy is to establish guidelines to ensure that Artificial Intelligence (AI) tools are used in a secure, responsible, and ethical manner.

The use of AI tools has the potential to enhance the quality and efficiency of the advice and services we provide. However, it is essential to ensure that these tools are used responsibly and ethically to maintain trust and confidence in the financial services industry and our business. By adhering to the principles outlined in this policy, you will be able to leverage AI tools/technologies to better serve clients while mitigating risks and ensuring compliance with both our business and regulatory requirements.

This policy is designed to ensure:

- AI tools are used ethically, fairly, and without bias.
- the impact of AI tools on our clients and our business is regularly assessed.
- AI is not used for illegal activities, harassment, or infringement of others' rights.
- transparency, accountability, and confidentiality are maintained in AI tool usage.
- the obligation to act honestly, efficiently, and fairly is complied with.

Scope

This policy is a guide for employees, representatives, contractors, and third-party partners of Insight Investment Partners on how to be safe and secure when using AI tools, especially when it involves the sharing of potentially sensitive company and client information.

The words "we", "us" and "our" are used to refer to Insight Investment Partners. The words "you" and "your" refer to Representatives/Advisers/employees.

Background

AI tools are transforming the way we work. They have the potential to automate tasks, improve decision-making, and provide valuable insights into our operations. However, the use of AI tools also presents new challenges and risks particularly in terms of information security and data protection.

The term AI (Artificial Intelligence) describes several algorithmic technologies such as machine learning, neural networks, computer vision, and robotics to perform human-like tasks such as reasoning, planning, natural language processing, computer vision, robotics and more.

"Generative" AI (such as ChatGPT/Copilot) generates new content such as images, text, software code or even music using algorithms and machine learning techniques.

AI systems can improve their performance over time according to a set of human-defined objectives and can operate with a certain level of autonomy.

AI and Financial Services

AI has been making significant advancements to many industries, including financial services. By embracing the power of AI, it may allow us, you, and our businesses to unlock new horizons by enhancing operational efficiency, improving client communication, and fostering new business growth.

Through the careful use and application of AI, it may assist us to spend more time with clients, less time on repetitive tasks, and ultimately, serve as a powerful growth driver across the financial services industry overall.

We recognise that while the use of AI tools can create benefits, they also pose risks to our operations and clients, including very real concerns around client privacy. Therefore, we are committed to protecting the confidentiality, integrity, and availability of all business and client information as a priority.

In addition, it is also important to strike a balance between automation and the human touch that clients will always need and value from their personal interactions with us. Whilst the use of AI tools can help drive growth and efficiency, as well as compliment the human experience for clients, it is important to remember that we are ultimately responsible and accountable for any advice and services provided to clients.

Guiding Principles in using AI

The following are the guiding principles that Insight Investment Partners will use in governing the way in which we adopt, use, and oversee the use of AI in our business:

- We will respect data privacy, security and confidentiality when using AI
- AI will be used to drive efficiency; but reliability and accuracy of outcomes will be up to us
- AI systems we utilise will be fair and unbiased, avoiding discrimination or unfair treatment of individuals or groups
- We will use AI to complement, not replace the human experience and human judgement

Benefits of AI

Some ways in which AI can be used to improve efficiency, business operations and engagement with clients includes (but not limited to):

Enhanced efficiency: AI tools can assist with automating repetitive tasks such as portfolio management and client communication, allowing you to focus your time and energy on higher-value activities such as personalised client interactions and strategic decision-making.

Content creation: AI tools can assist with generating content for various mediums such as websites, social media channels, and marketing materials. This can save time and resources while still producing high-quality content that is engaging and informative.

Client Engagement: AI tools can be used in several ways such as using a chatbot to engage with clients on social media platforms. Such tools can also be used to generate responses to client email/enquiries which can help improve client satisfaction and loyalty.

Research and analysis: AI tools can be used to analyse client enquiries, feedback, or reviews to identify common themes or issues. This can help us make decisions regarding improvements and/or opportunities, as well as improve the services we offer clients.

AI Tool Classification Framework

Tier 1 – Approved (Client Data Permitted)

Tools that have been assessed and approved for use with identifiable client data.

Private AI Tools
iComply2 SARA – Statement of Advice Review Assistant
iComply2 Finley
Business/Microsoft365 Co-pilot
Paradino
Claras ai
FileNotes.ai
Marloo

Tier 2 – Limited Use (Anonymised Data Only)

Public AI tools that may be used with **strict** controls.

Public AI Tools
ChatGPT (OpenAI)
Claude (Anthropic)
Grok (xAI)

Conditions:

- Data is not used for model training
- Zero data retention
- Security and privacy controls
- Read and understand **Lesson 5 - AI Tool Privacy: Chat Controls and Opt-Out Obligations** in full

STRICT REQUIREMENTS:

- **No identifiable** client or business information must be entered
- Any confidential and identifiable data **must be fully anonymised or removed**
- **Redaction alone is not permitted**, as masked or hidden data may still be recoverable or interpretable by AI systems

  EXCEPTION: Controlled Redaction using Adobe Acrobat Pro

  Redaction may be used as an alternative to anonymisation ****only when performed using Adobe Acrobat Pro's official Redact and Sanitize tools**** as follows:

  - Redaction must be applied using: **"Redact a PDF" → Mark for Redaction → Apply** (ensuring permanent removal of underlying data)
  - The **"Sanitize Document" / "Remove Hidden Information"** removes hidden data from PDFs including metadata, embedded content, scripts, and other non-visible elements that could contain sensitive information or pose security risks.
  - The redacted document must be saved as a **new file** (original version retained separately)
  - Users must verify that redacted content cannot be copied, searched, or recovered prior to AI submission
  - Manual or visual redaction methods (e.g. shapes, black boxes, highlights) remain **strictly prohibited**
  - Read more about Redacting/Sanitizing data here: https://helpx.adobe.com/acrobat/desktop/protect-documents/redact-pdfs/redacting-sanitizing.html

Examples of Anonymisation Techniques:

- *Replace names with generic data (e.g. "Jimmy Test", "Kelly Test")*
- *Replace addresses with generic values (e.g. "123 Street")*
- *Replace account/policy numbers with dummy values (e.g. "123456789")*
- *Replace contact details with fictitious data (e.g. "0456789123", "testclient@gmail.com")*
- ***Remove** any fields that cannot be effectively anonymised*

Examples of Identifiable Prohibited Input:

- *Names, dates of birth, addresses, TFN, contact details*
- *Financial account details (e.g. account numbers, policy numbers)*
- *Portfolio specifics linked to identifiable individuals*

Tier 3 – Restricted (Approval Required)

AI tools not yet assessed.

Requirements:

- Completion of AI Risk Assessment. See Appendix 1: Sample Risk Assessment Form
- Approval from Compliance before use. Email support@insightmp.com.au or support@iip.net.au for assessment and approval.

Tier 4 – Prohibited

AI tools that:

- Retain or train on input data without control
- Have unclear data ownership or security
- Operate in high-risk jurisdictions without safeguards

Requirements and Best Practice When Using AI

When using AI tools, you are required to comply with the following guidelines that have been put in place to protect our business, you, and our clients:

Requirement	Description	What this means

Product Risk Assessment	You must undertake a risk assessment of the tool prior to use.	• New AI tools must be assessed for, as a minimum:
		  ○ Cyber & data security risks
		  ○ Financial costs
		  ○ Legal contract terms (including data ownership and storage)
		  ○ Compatibility with existing systems and processes
		  ○ Sustainability, location, and reputation of the vendor
		  ○ Ethical implications
		• A **Risk Assessment Form** will be completed for each AI tool.

Privacy	As AI relies on vast amounts of data, you must handle sensitive client and business information securely and it must comply with privacy regulations (such as the Australian Privacy Principles).	• You must not disclose, upload, or share client or business information on Public AI. Disclosure must meet **Tier 2** conditions above. • Our use of AI tools must align to our Privacy Policy. • Any suspected privacy breaches must be reported **immediately**.
Transparency	Clients should be informed about the use of AI in our advice and services and understand its implications for any financial advice provided to them. You should also ensure clients have sufficient knowledge to make informed decisions about the use of AI.	• Where AI-generated content is used in the provision of financial advice, this will be disclosed to clients. • Where AI is used to record Personal Identifiable Information (PII) – e.g. file notes /needs analysis, this will be disclosed to clients.
Ethics & Fairness	AI tools can only be used in ways that uphold the highest ethical standards. You are responsible for implementing measures to prevent biases and discrimination in AI outcomes. You should be aware of biases and try and mitigate at every opportunity.	• Where you identify any errors/biases in AI tools, you must report it immediately. • AI tools will be reviewed and audited by the Compliance Manager on a regular basis to identify and rectify biases. • Where AI tools are used to support the provision of personal advice, the principles of the Code of Ethics will prevail.
Oversight	Always balance efficiency with human oversight. Monitor and review AI generated material, e.g. file notes, marketing materials, recommendations etc.	• You and/or we are accountable for any recommendations and decisions made using AI tools. • You must ensure that any advice recommendations align with the clients' best interests and must not be misleading or deceptive.
Accuracy	You must ensure content is accurate and it must be checked for spelling/grammatical errors as well as well-written in a way that is coherent, personalised (where relevant) and engaging.	• All AI-generated content must be proofread and checked by you, or peer reviewed by someone in the business. • Any sources used must be verified and any claims that are made must be supported by evidence.

Requirement	Description	What this means
Monitoring	You must stay updated on AI developments and review/update the use of it in our processes accordingly. Regular training and education are also necessary to navigate the ever-changing landscape of AI technologies.	• Approved AI tools will be monitored on an ongoing basis to ensure it's being used in line with our Guiding Principles. • AI tools will be regularly monitored for changes and to assess their continued effectiveness and assessed to identify any of new risks. • Where AI is used in critical business activities, it will be monitored on a regular basis.
Misuse	You must not use AI tools for illegal activities, harassment, or actions that infringe upon others' rights. Mishandling client data through AI tools can constitute a breach of your obligations under the Corporations Act 2001 (Cth), the Privacy Act 1988 (Cth), and the Licensee's compliance framework. Non-compliance may result in disciplinary action or licence consequences.	• You are required to report any misuse of AI tools **immediately**.
Record Keeping	You must maintain accurate records of the use of AI tools.	• Data inputs, "tree of thoughts" (e.g. the decision tree/process used) and any other relevant information, must be documented and retained on file, when used for the provision of personal advice. • Where AI tools are used in the provision of personal advice, records must be kept in the client file for a period of 7 years.

Appendix 1: Sample Risk Assessment Form

<Name of AI Tool>	
Description & Use	Please describe the AI Tool and what you will use it for, including pain points its use will alleviate (e.g. such as Chat GPT, which is used for marketing purposes, articles, LinkedIn posts, blogs, etc).
Vendor/Business Details	Details such as company name, website of the provider, link to privacy policy of company, including whether it is part of existing technology (e.g. AI assisted file notes via Microsoft Teams) or new technology.
Reviewer	<Insert Name>
Date of Review	<DD/MM/YY>

Topic	Details, information reviewed or comments	Internal Risk Assessment (appropriateness based on our requirements, AI policy and internal standards)
Cyber & Data Security Risks		☐ Internally assessed to be appropriate ☐ Not acceptable to use
Ongoing Financial Costs		☐ Internally assessed to be appropriate ☐ Not acceptable to use
Legal contract terms (including data ownership and storage)		☐ Internally assessed to be appropriate ☐ Not acceptable to use
Compatibility with existing systems, processes and policies (including Privacy Policy)		☐ Internally assessed to be appropriate ☐ Not acceptable to use
Sustainability, location and reputation of the vendor		☐ Internally assessed to be appropriate ☐ Not acceptable to use
Ethical implications / biases		☐ Internally assessed to be appropriate ☐ Not acceptable to use

Outcome	
Result:	Approved or Not Approved
Date Approved:	<DD/MM/YY>
Approver:	<Insert Name> - Director/Risk & Compliance Committee

Appendix 2: Sample Process for Assessing New AI Tools

This process will be used to assess new AI tools