Licensee Standard
TECHNOLOGY, AI AND OVERSEAS DATA

Version 1.0

AIM

This Licensee Standard will assist you to:

- Understand what technology systems are approved for use and the process for conducting due diligence on providers of systems and AI tools.
- Understand the requirements if technology systems and AI tools store or transmit client data overseas
- Understand the requirements for the ethical, secure, and effective use of Artificial Intelligence (AI) Tools

APPROVAL PROCESS FOR TECHNOLOGY

Centrepoint encourages practices to use technologies that will suit their business needs provided appropriate records are kept in Xplan (Compass/CWT) in line with the Record Keeping Licensee Standard. SoAs should be produced through Compass/CWT and Adviser Logic only.

Approvals are not required for:

- specific operating systems (e.g. Windows, macOS)
- general office suites (e.g. Office365, Google Workspace)
- general business applications (e.g. Xero, Lucidchart, Adobe).

To facilitate adoption of new technology, Centrepoint has reviewed and pre-approved a range of technology systems and AI tools. Refer to the Technology Solutions Hub Technology Stack for the current approved technology and AI tools.

Approved Provider

Centrepoint has undertaken system data security checks, tested and integrated the software. Centrepoint perform due diligence on the reliability of projections, input approved rates, and update the templates/systems. These systems and tools meet our data and security requirements, including compliance with overseas data guidelines (if applicable).

Security Approved

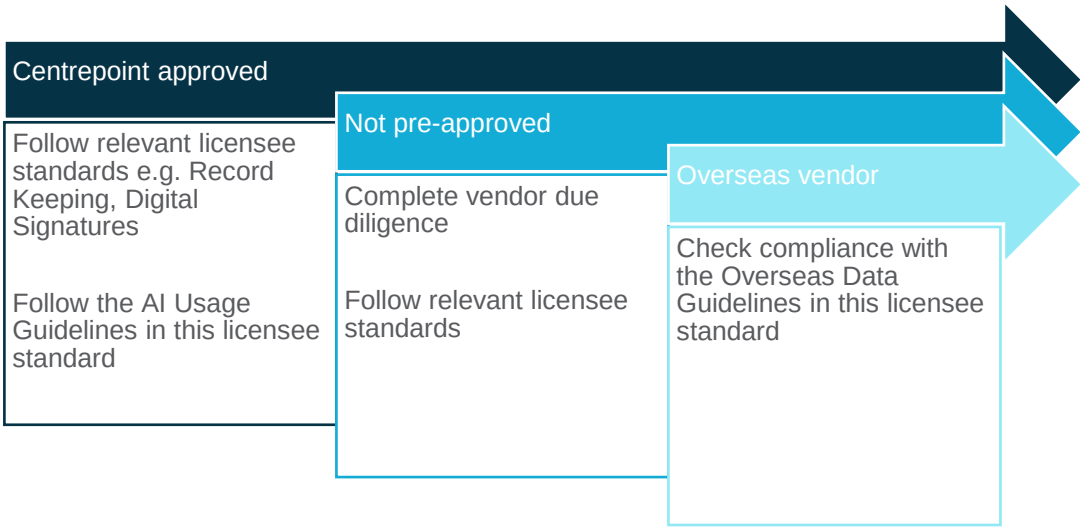
For these systems Centrepoint undertake system data security checks but the practice is responsible for set up, testing and integration.

Centrepoint has also pre-approved AI tools that meet our data and security requirements, including compliance with overseas data guidelines (if applicable).

Not pre-approved

Should you wish to use technology or AI that is not listed as approved by Centrepoint, you should undertake due diligence to evaluate third-party systems for compliance with privacy obligations and data and cyber security. This due diligence should also include (if applicable) ensuring that overseas vendors adhere to data protection agreements that meet Australian privacy laws or the countries they operate in have been prescribed by the Minister as having similar privacy laws to Australia.

We have provided a Vendor Due Diligence Questionnaire (including checking compliance with overseas data guidelines) in the Appendix.



WHAT IS ARTIFICIAL INTELLIGENCE?

Artificial intelligence (AI) is a collection of technologies, such as machine learning, deep learning, and natural language processing that can be used to solve problems autonomously and perform tasks to achieve defined objectives.

AI is a rapidly evolving technology that has the potential to transform the financial services industry and improve outcomes for consumers and investors. However, AI also poses significant risks and challenges, such as ethical, legal, and regulatory issues, as well as potential impacts on trust, accountability, and human oversight.

AI use by advisers

AI is generally used within practices to assist or augment human decision making or increase efficiency, rather than make autonomous decisions. Examples include generating drafts of documents, file notes or correspondence.

AI introduces new or additional obligations and challenges for financial advisers, such as ensuring the accuracy, reliability, and explainability of the AI system, as well as the protection of the data and privacy of the clients.

Common AI tools

Requirements	
Filenote.AI	Filenote.AI is a Centrepoint preferred AI tool. It is approved and meets data and security requirements. Filenote.AI takes the data from your environment transfers it to an Australian based data centre. It undertakes the transcription and then deletes the data from their server.
Microsoft Copilot	Microsoft Copilot is a Centrepoint preferred AI tool. It is approved and meets data and security requirements. Microsoft Copilot retains data within your Microsoft tenancy and on Australian based servers. Data is not used to train large language models (LLMs). Copilot allows you to retain all the information within your corporate environment meaning that it can be used on private and confidential information safely.

Requirements	
ChatGPT	ChatGPT is not currently an approved Centrepoint AI Tool. However, we understand that many practices use the tool in their businesses. If you are using ChatGPT we recommend that you: 1. Only use the paid version of ChatGPT for business purposes; 2. Anonymise data; and 3. Opt out of the data being used to train and improve the model. You should be aware of the following when using ChatGPT: • ChatGPT collects and stores user interactions to improve its services. This includes prompts, responses, and usage data. • Data from ChatGPT interactions may be used to train and improve models unless users opt out. • The paid versions offer enhanced features and support but follow similar data handling practices as the free version.
Free AI tools	Generally, if the tool is free, it is unlikely to meet data and security requirements and should be used with caution and only using anonymised data. This involves removing identifiers like names, address, phone numbers, and other information that can be used to reveal someone's identity such as account details.

AI USAGE GUIDELINES

Requirements	
Use guidelines	Identify where AI is being used in the business. Define and document how AI can be used within the practice, including the purpose and AI tools. Include future plans for AI use. Review and update before implementing new AI systems or uses. While it is often not practical, or possible, to understand the intricacies of how AI systems work, it is still important to understand their general limits and constraints. This ensures that you are aware of the risks, vulnerabilities, reliability of outputs, and optimise its usage.
Client consent	Obtain explicit consent from clients before using AI tools. Communicate how you will use AI and allow client to opt-out. For example, if you are using a transcription service, you should disclose this to the clients prior to recording the meeting and obtain their consent. Consent should be recorded in file notes.
Training	Ensure staff are trained on AI usage policies, data privacy, and security. Train staff on the functionality and limitations of AI tools used in the practice. Staff that use AI systems should be trained on what data can and cannot be input to the system, for example, personally identifiable information or the organisation's intellectual property. Staff should also be trained on the extent to which the system's outputs can be relied upon.
Fact checks	Always fact-check the information generated by AI Systems. Do not solely rely on it; instead, use your own judgment and expertise to assess its accuracy, potential bias, and relevance.
Anonymisation of personal information	Personal identifiers should be anonymised or pseudonymised where possible and if appropriate to safeguard individual privacy and reduce risk exposure. Avoid copying client's personal information into AI Systems **unless** the system retains the information within Australia and does not use this information to train the AI model. However, we recommend using an approved system that allows you to use the AI tool knowing that the data is kept secure and personal information is safeguarded without the need to anonymise.

Requirements	
Proprietary and confidential information	Inputs may be used to retrain the AI system's model and may be available to other users. Avoid copying any company proprietary, third-party proprietary, or confidential information into AI systems **unless** the system retains the information within Australia and does not use this information to train the AI model, or it is an approved system. Proprietary and confidential information includes intellectual property, policies, contracts, financial data, and client lists.
Ongoing compliance	Identify and manage risks associated with AI by periodically reviewing your AI usage and procedures to ensure compliance with the requirements in this licensee standard.

OVERSEAS DATA GUIDELINES

Requirements	
Australian Privacy Principles (APP)	Advisers are required to collect, store and use data in accordance with APPs. Before you commence using the services of an overseas service provider (e.g. Otter, Fireflies, Loom) you must take reasonable steps to ensure the provider does not breach the APPs in relation to the information.
Exceptions	Privacy and Other Legislation Amendment Bill 2024 enables overseas disclosure of personal information to countries with similar privacy laws and protections. Where a jurisdiction is prescribed, a Practice does not need to take steps to ensure that the offshore recipient does not breach the APPs. There are currently no countries on this list. Practices must still undertake appropriate due diligence, obtain client consent and ensure data and cyber security requirements are adequate.
Contracts	The adviser firm should enter a contract with the overseas third-party provider which covers such things as: • Privacy and data protection clauses. These must include confidentiality, security, and compliance of the personal information and provisions that the overseas third-party entity must adhere to the APPs and not breach the APP requirements. • A data transfer agreement that includes provisions ensuring the third party's adherence to Australian privacy standards. • the undertaking of regular reviews of the provider's compliance and performance for adherence with the APP requirements, and • How the provider will deal with breaches or data security breaches.
Overseas Privacy Disclosures and Consent	The APPs state that an entity's Privacy Policy must include information about whether the organisation is likely to disclose personal information to overseas recipients and, if so, the countries in which such recipients are likely to be located. Centrepoint's Privacy Policy states that Advisers will make these disclosures to clients. The Practice must seek explicit consent from the client to use and share their personal information with an overseas entity and inform the client of the nature and scope of the services that the provider will offer. This must be to provide services in line with the primary purpose for collection of the data i.e. the provision of financial advice and services. The Practice must make this disclosure and obtain consent, for example by using the Fact Find Client Declaration. ☐ I give permission for the information provided in this Fact Find and related documents to also be disclosed to the following people/parties (e.g. name of my spouse/solicitor/accountant/offshore provider including country

Requirements	
Managing data breaches	The Practice should establish a process for managing data breaches or incidents involving the third party.

RESOURCES

ASIC and the Government have also released several guidelines pertaining to the use of AI.

- Australia's AI Ethics Principles
- Voluntary AI Safety Standard August 2024
- Proposals paper for introducing mandatory guardrails for AI in high-risk settings. Sept 2024
- Australian Responsible AI Index 2024 Sept 2024
- Policy for responsible use of AI in Government. Sept 2024
- Beware the gap: Governance arrangements in the face of AI innovation - ASIC Report 798 October 2024

QUERIES & FURTHER INFORMATION

Additional queries should be directed to professionalstandards@cpal.com.au or Advice Technology on 1300 557 598.

Version	Date	Changes
1.0	24/03/2025	New

APPENDIX

Technology/AI Vendor Due Diligence Questionnaire

Due Diligence Checklist	Responses
Name of provider/software	
What does the software do and what is its intended use?	
Is it a Centrepoint security approved software/AI tool? If no, is there a Centrepoint approved provider or security approved provider that could be used for this purpose?	
About the provider/system	
Is the business well established or do the people involved have sufficient years of experience? How many employees work in the business?	
Does the provider have experience working with financial services businesses?	
Who uses the system? Are there other clients similar to your business in size and needs? Are there references or can you speak to other clients?	
Does the system integrate with our existing systems?	

Due Diligence Checklist	Responses
Does the system integrate with Xplan? If it does not integrate how will data and records be input into XPlan?	
What other providers/software have been considered? Why was this chosen?	
Privacy and Data Location	
Is our data used to train and improve AI models? If yes, can we opt-out?	
Is our data retained within Australia? How is data managed by the provider and where is the location of the data?	
Does the provider have a Privacy Policy? Does the provider adhere to the APPs?	
Are any of the activities or services provided outside of Australia? If yes, which activities and where?	
Will our data be replicated to another country or state in any way? If yes, does the provider's contract contain appropriate protections?	
Governance	
Does the provider have a governance, compliance and risk framework?	
Does the provider have a business continuity plan (BCP)? If yes, when was it last tested and what were the results?	
Does the provider have a disaster recovery plan (DRP)? If yes, when was it last tested and what were the results?	
Does the provider deliver Cybersecurity and Privacy Awareness training to its staff? If yes, what is the frequency?	
What certifications does the provide have e.g. ISO standards? ISO27001 certification is the international framework that demonstrates a certain level of legal, physical and technical controls.	
If credit card information is stored, is the provider Payment Card Industry Data Security Standard (PCI DSS) compliant?	
Does the provider have cyber insurance? If yes, provide details of the policy.	
Information and Data Security	
Does the provider have an IT and Data Security Policy? If yes obtain a copy. Does the policy include, and/or can the provider explain and evidence the following:	

Due Diligence Checklist	Responses
• System security measures • Reasonable steps to ensure that personal information it holds is protected against misuse, loss, corruption and from unauthorised access (e.g. network security, monitoring of employee email activity, anti-virus software, firewall infrastructure, penetration testing, monitoring of access, user access revalidation to key system), modification or disclosure.	
Is data backed up?	
What encryption is in place for data at rest, in transit and back up?	
Are penetration tests performed by a qualified third-party vendor? If so, how often are they performed and when was the last test performed?	
What physical security controls does the provider have to protect client information and prevent unauthorised access to information?	
Does the provider have a Data Breach Response Plan? What is the process for managing data breaches?	
Risks and Security Breaches	
Has the provider been subject to an internal or external IT audit review in the past 12 months? Have any issues from this review been remediated?	
In the last 12 months, has the provider had any instances where the Physical Security Controls or IT Security controls were breached by an internal or external malicious user? If yes provide details of the breach and any preventative measures implemented.	
What liability will the provider accept for data and cyber issues?	
Contract Considerations	
What is the length of the contract?	
Is the pricing appropriate?	
What support and training will we receive from the provider?	
What are the agreed service levels and how will they be measured? How responsive is the provider to queries or concerns?	
Are there appropriate termination clauses in the contract in relation to material defaults, non-provision of services, change of control or breach of contract?	

Due Diligence Checklist	Responses
Are there any conflicts present, e.g. joint ownership, directors, and related business and how would they be managed?	