

CHR032 AI (Artificial Intelligence) Policy

Overview

Catena recognises that the use of AI (Artificial Intelligence) has grown and is now a widely used tool, and the company promotes and advocates the use of AI in a measured and controlled manner.

AI tools can enhance services by automating routine tasks, enhancing data analysis, speeding up information retrieval and aid creativity, however this comes with its own set of risks and it is important that we set clear guidelines on how and when this technology may be used.

This policy sets out user responsibilities when using AI tools and aims to ensure:

- data protection and information management processes are followed
- user accountability for AI usage
- accuracy of information generated by AI tools
- transparency when using AI tools
- Use for online meetings

Purpose

This AI policy establishes end user responsibilities when using AI tools for official Catena business. The policy aims to ensure that AI tools are used securely by outlining acceptable use of AI, the need to check accuracy of results, the need for transparency and user accountability for AI generated content. The policy also addresses the data protection responsibilities of users when utilising AI tools.

This policy applies to:

- All Catena employees (whether permanent or temporary)
- Suppliers and subcontractors to Catena
- All AI tools including but not limited to, generative AI, machine learning and large language models

Third Party Compliance

a) Suppliers and their third parties, whether permanent or temporary, have security responsibilities and must be aware of and comply with Catena's AI policy.

b) All actual or suspected security incidents and data breaches must be raised with Catena's IMS Manager.

c) Catena reserves the right to assess for compliance with this policy and may request to inspect systems, information and documentation to facilitate this.

d) If for any reason suppliers and their third parties are unable to comply with this policy or require use of technology which is outside its scope, they must discuss this with the contract manager who must then contact the IMS Manager to discuss a possible exception to policy.

Examples of Acceptable AI Use

- **Content Drafting** - From a description or Catena supplied material, such as brainstorming marketing material, creating blog posts, summarising and comparing publicly available documents.
- **Data Analysis** – Using Catena produced statistics or publicly available data as long as it's fully anonymised
- **Minute Taking in meetings** – where all participants agree and where the subject matter is not classified as Official or above. This is never permitted in a Rolls Royce meeting

Examples of Prohibited AI Use

- **Data Uploads** – You must not submit personal identifiable data, client records or financial data into public AI platforms (e.g. ChatGPT, Claude etc)
- **Customer Supplied Information** – Documents supplied from outside of Catena such as Project Briefs, Drawings and Identifiable Data must never be submitted into a public AI platform.
- **Automated Decision Making** – AI must never be used to make a decision, and all outputs must be reviewed.
- **Minute Taking in Rolls Royce or RR Sub Tier meetings** – regardless of agreement

Meeting Recorders and Extensions

- **Automated Meeting Recorders:** Third-party AI bots (e.g., Otter.ai, Fireflies) are prohibited from joining meetings. If an unauthorized bot joins, the meeting host must remove it immediately. Catena may authorize the use of a specific program but even agreed programs must be set as a default to **NOT** join meeting automatically. Permission should be sought from the meeting host if it's not you, and if you are the host, and the meeting is not RR related, you may ask permission from other attendees to use the meeting recorder.
- **Browser Extensions:** Installing browser extensions that use AI features is prohibited. These extensions often require full read-access to web traffic, including private emails and banking portals.

Data Classification Protocol

You must classify data **before** entering it into any AI tool. Use the table below to determine what is safe.

CLASSIFICATION	AI RATING	DESCRIPTION	REQUIREMENTS	EXAMPLES
PUBLIC DATA	 SAFE	Information already available in the public domain.	No restrictions.	Marketing copy General industry research Brainstorming
INTERNAL DATA	 CAUTION	Internal business documents that are not confidential.	Anonymization Required.	Internal Memos Process Documentation Draft Emails
RESTRICTED DATA	 PROHIBITED	Any data that would cause harm if leaked.	NEVER input into AI.	PII: Client Names, SSNs, Home Addresses Financials: Bank Accts, Credit Cards Credentials: Passwords, API Keys

Unsure about a document?

If you are ever unsure about how to classify any data or document, get in contact with either the IMS Manager or the Managing Director so we can perform a Data Classification Review.

AI Hallucinations and Output Verification

AI models frequently "hallucinate", and when they do, they confidently present incorrect information as fact.

You are required to fact-check 100% of AI-generated claims against a primary source.

Never rely on AI for:

- Legal Statutes or Case Law.
- Mathematical Calculations.
- Factual citations or historical dates.

If you make a business decision based on AI output, you must validate the data first.

Voice Cloning and Deepfakes

The use of AI to clone, simulate, or mimic the voice or likeness of any human being (including staff, contractors, suppliers, or public figures) is strictly prohibited unless explicitly authorized in writing by Company Leadership.

This includes using "Text-to-Speech" tools that are trained on a specific individual's voice samples.

Financial Verification

Deepfake technology is now used to commit wire fraud.

Any urgent request for funds (wire transfers, gift cards, invoice payments) or credential changes received via voice, video, or email requires secondary verification.

If you get a call from the "CEO" asking for money, hang up. Call them back on their known internal phone number to verify the request.

AI-Assisted Decisions

AI tools lack human judgment, ethical reasoning, and real-world context. They frequently "hallucinate" (invent facts) or rely on biased training data while sounding completely authoritative.

Relying on AI as the only decision-maker can lead to disastrous outcomes. A single unverified AI decision can result in wrongful termination lawsuits, flawed investment strategies, regulatory fines, and serious damage to our client relationships and brand reputation.

A human must review and approve **ALL** "AI-Assisted Decisions." This applies to any professional judgment, including but not limited to:

- Hiring and Termination decisions.
- Employee performance evaluations.
- Financial approvals.
- Strategic business planning.
- Professional Advice (Legal, Medical, Financial).

Transparency and AI-Assisted Generation

Transparency is key to maintaining client trust.

- **External Disclosure:** If AI is used to generate any content for a deliverable (e.g., a report, code module, image, or article), you should disclose the use of AI to the client
- **Internal Disclosure:** When submitting work to a manager, you must flag if the content was "AI-Assisted Generation" to ensure proper review.
- **Watermarking:** Where technically feasible, AI-generated images should keep their metadata or visible watermarks indicating their artificial origin.

Mobile and Personal Device Usage (BYOD)

The use of AI apps on personal devices to work on company tasks is prohibited.

- You may not copy company emails, files, or chat logs into AI apps (e.g., the ChatGPT iOS/Android app) on a personal device.
- Mobile access to AI tools is only permitted via approved apps.

Incident Management and Roles and Responsibilities

We value a culture of trust and security. These guidelines are here to protect you, our clients, and the company's reputation. We understand that mistakes happen, but wilful disregard for these safety measures—such as bypassing security controls or sharing sensitive data—is a serious issue.

If a violation is detected, we will investigate the circumstances. While accidental errors (especially those that are self-reported) are often treated as learning opportunities, deliberate violations or negligence will be met with appropriate disciplinary steps.

Breaches or suspected breaches of this policy shall be reported to the Managing Director or the IMS Manager – this can be done under the Whistle Blowers Policy if required.

Definitions

Artificial intelligence (AI) - A computer programme which 'learns' from data and may perform tasks usually carried out by humans.

AI tool - Any computer software that uses artificial intelligence in its processing.

Approved AI tools - AI tools that reside on the Catena infrastructure and that have been approved

Online AI tools - AI tools which are accessed on the internet through a web browser.

AI output - Any content that is generated by an AI tool.

Generative AI - A form of AI which generates content based on the inputs of users.

Large Language Model - A form of generative AI that examines very large datasets to produce context related output.

Prompt - An instructive command or question which directs AI to perform tasks.

Machine Learning - A form of AI which self learns without following explicit instructions.