MICKAI™

MICKAI EBOOK SERIES · PLAYBOOK No. 8

What is AI? A plain-English, substrate-first introduction.

An introduction for the UK SME owner, board member, and engineer. The technology, the failure modes, the policy layer, and the substrate underneath that decides whether any of it is verifiable.

AUTHOR

Micky Irons

Founder and named inventor, Mickai LTD.
Crunchbase · LinkedIn · GitHub · mickai.co.uk

DATE · 17 May 2026 · v1

EBOOK · No. 8 IN A SERIES OF 14

Mickai LTD · Companies House 17166618 · press@mickai.co.uk · mickai.co.uk

UK IPO register GB2607309.8 to GB2611702.8 and GB2611885.1 onwards · Trade mark UK00004373277

TABLE OF CONTENTS

Contents

Foreword

A note from the author

Part I · The Technology

1. What an AI model actually is
2. Training, inference, fine-tuning, agents
3. Where the model runs, who owns the keys

Part II · The Failure Modes

4. Hallucination
5. Prompt injection and jailbreak
6. Data leakage and shadow AI
7. Autonomous agent risks

Part III · The Policy Layer

8. UK GDPR, ICO, NCSC
9. PRA SS1/23 model risk
10. DSIT AI Cyber Security Code of Practice

Part IV · The Substrate Underneath

11. Why audit format is the trust root
12. Post-quantum signing, hash-linking, browser-resident verification
13. The procurement question every board should ask

Appendix

About the author
References and further reading

FOREWORD

A note from the author

AI is the technology category every UK board now has to make decisions about, without the engineering vocabulary to do it. This ebook is the plain-English introduction that explains what AI actually is, what its failure modes are, why the policy layer matters, and why the substrate underneath the policy layer is the variable that decides whether AI is verifiable in your organisation.

It is written for the UK SME owner, the non-technical board member, and the engineer who has been asked to brief the board next quarter.

The Mickai substrate primitives are filed at the UK IPO across the GB2607309.8 to GB2611702.8 and GB2611885.1 onwards families. The trade mark Mickai is registered at UK00004373277.

Micky Irons

Founder and named inventor, Mickai LTD · 17 May 2026

PART I · THE TECHNOLOGY

What AI actually is, in plain language

1. What an AI model actually is

An AI model is a large file of numerical parameters (weights) and a small piece of software (the runtime) that, together, transform a structured input into a structured output. The input might be a prompt; the output might be a response. The weights were learned by running a training process over a very large dataset; the runtime is what executes the learned function against new inputs.

The model itself is not magic. It is a deterministic mathematical function. The behaviour the user observes (responsiveness, creativity, the appearance of reasoning) is the function's output. The same model run twice on the same input under the same parameters produces the same output.

2. Training, inference, fine-tuning, agents

Training is the expensive, one-time process of learning the weights from a dataset. Inference is the cheap, ongoing process of running the trained weights against new inputs. Fine-tuning is a small additional training pass that nudges the weights for a specific domain or task. An agent is a wrapper around inference that adds memory, tool use, and multi-step reasoning to produce more autonomous behaviour.

For a UK SME, the practical decisions are about inference (where does it run, who pays per call, who holds the key) and agents (what can they touch, under what authority, with what audit trail). Training and fine-tuning are typically vendor concerns until the SME reaches significant scale.

3. Where the model runs, who owns the keys

The most consequential AI decision a UK board makes is not 'which model'; it is 'where the model runs'. Three options: vendor cloud (OpenAI, Anthropic, Google, Microsoft, AWS, etc.), vendor edge (the same vendor's hardware on premise), or operator iron (the SME's own hardware). Each option has different cost, latency, security, and regulatory consequences.

Who owns the key matters as much as where the model runs. The signing key for any audit trail decides who can produce the regulator-facing evidence at incident review. The vendor-owned key is a contractual position; the operator-owned key is a structural position.

PART II · THE FAILURE MODES

Where AI goes wrong, and how to recognise it

4. Hallucination

An AI model can produce plausible-sounding output that is factually wrong. This is hallucination. The model is not lying; it is sampling from its learned distribution and the sample happens to be unanchored to reality. Hallucinations are particularly dangerous when they appear in regulated contexts (legal, medical, financial) where downstream parties trust the surface authority of the output.

The mitigation is retrieval-augmented generation (RAG), where the model is grounded in a specific document corpus and asked to cite, and the chain-of-custody at the substrate layer (the OAR), where every grounding decision and citation is recorded for downstream verification.

5. Prompt injection and jailbreak

Prompt injection is when external content (a web page, a document, an email) contains instructions that an AI agent reads and acts on as if they came from the operator. Jailbreak is when an adversary crafts a prompt that bypasses the AI's safety training. Both are structural risks for any AI agent that touches untrusted content.

The mitigation is sandboxing (the Mickai Browser Brain's hybrid sandbox is one example), capability scoping (the agent cannot do what it is not authorised to do), and audit (every action is signed and the operator can replay).

6. Data leakage and shadow AI

Data leakage is when production data leaves the operator's perimeter through an AI tool. Shadow AI is when employees use AI tools the operator has not approved. Both are common in 2026 UK SMEs and are the primary mechanism by which sensitive data ends up on third-party servers.

The mitigation is data classification (what may leave the perimeter), enforcement (the network blocks unapproved AI endpoints), and substrate (operator-iron AI tools that satisfy the productivity demand without requiring egress).

7. Autonomous agent risks

An AI agent that can act in the world (send email, write code, transfer money, change settings) has all of the above risks plus the ability to actuate them. The 2026 record on autonomous agent failures is small but growing; the mitigation is the same substrate position: explicit capabilities, signed actions, replayable audit.

PART III · THE POLICY LAYER

UK regulation in plain language

8. UK GDPR, ICO, NCSC

UK GDPR is the data protection statute. The ICO is the regulator. The NCSC is the technical security authority. For any UK SME using AI on personal data, all three are in the regulatory picture. UK GDPR Article 22 covers automated decision-making; the ICO publishes practical guidance; the NCSC publishes technical guidance including the AI Cyber Security Code of Practice consultation.

9. PRA SS1/23 model risk

For UK SMEs in financial services, PRA SS1/23 governs model risk management. The supervisory statement sets the floor on model inventory, model validation, and model audit. SMEs above the relevant thresholds are required to demonstrate compliance; SMEs below the thresholds typically still adopt the principles voluntarily.

10. DSIT AI Cyber Security Code of Practice

The Department for Science, Innovation and Technology has consulted on a voluntary code of practice for AI cyber security. The code expects AI deployments to implement a baseline of security controls including capability scoping, audit logging, and supply chain assurance. UK SMEs adopting AI are encouraged to read the code as the de facto baseline regardless of statutory status.

PART IV · THE SUBSTRATE UNDERNEATH

Why the substrate decides whether AI is verifiable

11. Why audit format is the trust root

The substrate question is what format the AI's audit trail is in, who signs it, and who can verify it. Vendor JSON logs are unverifiable without the vendor. Hash-linked, post-quantum-signed records under operator key custody are verifiable independently. The substrate decision is upstream of the policy decision.

The substrate decides whether the policy can be enforced.

12. Post-quantum signing, hash-linking, browser-resident verification

The Mickai substrate produces, for any AI workload that wraps the decision-emit hook, a hash-linked chain of CBOR records signed under FIPS 204 ML-DSA-65 and verifiable through a browser-resident verifier. The board does not need to understand the primitives; the board needs to understand that the primitives exist and that the substrate produces the artefact the regulator will ask for at hour zero.

13. The procurement question every board should ask

The board's procurement question is: 'when the ICO or our sector regulator asks for the audit trail of any AI-assisted decision in our organisation, can we produce it without the AI vendor's cooperation, in a format the regulator can verify on their own laptop, signed under a key we control?' If the answer is no, the substrate is wrong, regardless of how good the AI is at its job.

Engineering leadership at any UK SME is open to a thirty-minute substrate briefing at any time. press@mickai.co.uk.

APPENDIX · ABOUT THE AUTHOR

Micky Irons

Founder of Mickai LTD (Companies House 17166618, England and Wales, registered office 20 Wenlock Road, London, N1 7GU). Named inventor on the Mickai SIOS patent corpus, recorded on the UK Intellectual Property Office public register at numbers GB2607309.8 to GB2611702.8 and GB2611885.1 onwards. Trade mark Mickai registered at UK00004373277 (classes 9 and 42, filed 15 April 2026).

Before founding Mickai, Micky was a Sellafield site worker. The egress constraint observed from inside the regulated workstation is the engineering origin of the substrate described across the Mickai ebook series.

Profiles and links

mickai.co.uk · the canonical Mickai site.

crunchbase.com/person/micky-irons · founder profile.

linkedin.com/in/mickyirons · personal LinkedIn.

github.com/Micky-CMO · open-source position.

linkedin.com/company/mickai · Mickai LTD company page.

crunchbase.com/organization/mickyirons · Mickai LTD Crunchbase entry.

Email: press@mickai.co.uk

Colophon

Set in Inter Tight (Variable) and Inter Black. Brand voice audited under the Mickai AMT preflight gate; zero violations at publish. © 2026 Mickai LTD. Reproduction permitted for internal procurement and engineering use within UK regulated organisations. External redistribution by written permission of the author.

References and further reading

· Information Commissioner's Office, UK GDPR guidance series.

· Information Commissioner's Office, AI and data protection guidance.

· PRA Supervisory Statement SS1/23, model risk management for banks.

· DSIT AI Cyber Security Code of Practice (consultation 2024 to 2025).

· NCSC, Timelines for migration to post-quantum cryptography.

· Mickai brain taxonomy: mickai.co.uk/brains.

· Mickai trade mark UK00004373277, classes 9 and 42, filed 15 April 2026.