CTOMETRY · FREE TOOL

AI Governance Policy — Starter

The six-page policy your board and auditors will actually read. Mapped to EU AI Act principles and ICO guidance. Adapt, don't adopt verbatim.

1. Purpose & scope

This policy defines how our organisation designs, procures, deploys and operates AI systems, and how we assure ourselves and our regulators that we do so responsibly.

2. Principles

• Human oversight of any AI-influenced decision that affects a person.

• Data minimisation — we use the least data required for the outcome.

• Transparency — users are told when they are interacting with AI.

• Accountability — every AI system has a named owner and a review date.

• Fairness — we test for and mitigate discriminatory outcomes.

3. Governance structure

Body	Remit
Executive sponsor (CTO/COO)	Owns AI strategy and register
AI Governance Group	Reviews use-cases, approves risk ratings
Data Protection Officer	Reviews personal data uses
Information Security	Reviews vendor & model risk

4. Controls

• AI Use-Case Register maintained and reviewed monthly.

• Approved AI Tools Register published and enforced.

• High-risk use cases require documented DPIA and human-in-the-loop.

• Vendor DD includes training-data provenance and data-use terms.

• Annual internal audit of AI controls; findings tracked to closure.

5. Prohibited uses

• Fully-automated decisions on employment, credit or benefits.

• Any use of personal data in consumer AI tools without approval.

• Any use of a model without documented provenance and terms.

When this workbook surfaces something worth acting on, book a Diagnostic Call at ctometry.co.uk.