

AI governance pack

Eight working documents for a 5–30 person regulated firm — most of them a page or less. Type directly into the boxes (this PDF is fillable in any reader), save a copy per review, and revisit annually or after any significant new tool. The reasoning behind every item is in the [AI governance series at cordrey.co](#).

This template is for informational purposes only and does not constitute regulated financial advice, legal advice, or a compliance opinion. Adapt it with a qualified compliance professional.

FIRM	COMPLETED BY	DATE
------	--------------	------

01 AI register

Every AI tool in use — including the unofficial ones. Reviewed quarterly; anything not on this register is not approved. (~1 page)

TOOL & VENDOR	USED FOR	DATA IT TOUCHES	CLIENT-FACING?	APPROVED BY / DATE
---------------	----------	-----------------	----------------	--------------------

02 **AI use policy — outline (2-3 pages)**

Draft the four sections below; the boxes hold your one-line summary of each, the policy itself lives in your document system.

Approved tools and uses. The register is the whitelist; the approved use per tool.

Prohibited uses. At minimum: client personal data in unapproved consumer tools; unreviewed AI output reaching clients; AI-generated suitability or advice determinations.

The review-before-use rule. Which outputs require human review, by whom, before they leave the firm.

Proposing new uses. How staff request a new tool or use, and who decides (item 03).

03 **Named owner**

One senior manager owns AI use — Statement of Responsibilities updated, approval authority documented in the policy.

ACCOUNTABLE SENIOR MANAGER	ROLE / SMF	SoR UPDATED? (DATE)	APPROVAL AUTHORITY DOCUMENTED?
----------------------------	------------	---------------------	--------------------------------

04 DPIA prompts — per tool processing client personal data

A DPIA that could describe any firm's use of any tool is not worth doing. One copy of this block per tool; name the specifics.

QUESTION

YOUR ANSWER

Which tool, and which categories of client data does it process?

Where is the data processed and stored (regions)?

Does the vendor retain inputs? Train models on them?

Lawful basis for the processing?

Automation classification: assistive with meaningful human review, or approaching solely automated?

Privacy notice updated to reflect this processing?

05 Vendor due-diligence note

One page per material vendor; refreshed at renewal.

QUESTION

YOUR ANSWER

Where does client data go, and is it used for model training?

Data residency and certifications held?

What model underlies the product?

What happens to our workflow if the vendor swaps models, reprices, or discontinues?

Exit: how do we get our data out?

06 Monitoring record

Sampled reviews of AI-assisted outputs — your Consumer Duty outcomes evidence, feeding the annual board assessment.

DATE	OUTPUT SAMPLED	AI INVOLVEMENT	FINDING	FIX / ACTION	REVIEWER
------	----------------	----------------	---------	--------------	----------

07 Audit-trail convention

The agreed one-line note recording AI involvement on each client-facing output — which tool, what it produced, what the reviewer changed, who approved. Agree the format once; use it every time.

FIELD	CONVENTION IN THIS FIRM
-------	-------------------------

08 Incident playbook (two paragraphs)

Write these now, not during the incident.

If a material AI vendor fails (outage, degraded output, security incident) — who is told, which processes revert to the documented manual fallback, who owns client communication:

If an AI-related data incident occurs — who assesses whether notification thresholds are met, and who calls the ICO (or your local supervisor); name the person and the deputy:

Want this mapped to your firm?

A discovery call is free and without obligation: bring this pack, and leave knowing which items you already satisfy and which need an afternoon's work. [Book a discovery call](#) · cordrey.co/contact · the series behind this pack: cordrey.co/knowledge/ai-governance

Review cadence: annually, and after any significant new tool. The regulation pages behind this pack are maintained at cordrey.co/knowledge — check their last-reviewed dates.