DEN AGENTIC AI · POLICY TEMPLATE

Responsible AI Use Policy Starter Template

A starting framework for building internal AI use policies. Covers acceptable use, approved tools, data sharing rules, output review, and human accountability. Customise highlighted sections for your organisation.

⚠ This template is a starting point only. Have this document reviewed by legal counsel before finalising and distributing to staff.

POLICY DOCUMENT DETAILS — COMPLETE BEFORE DISTRIBUTING

ORGANISATION NAME	POLICY OWNER / ROLE	EFFECTIVE DATE	REVIEW DATE

1 Purpose & Scope

This policy governs the use of artificial intelligence (AI) tools by employees, contractors, and partners of [Organisation Name]. It applies to all AI tools used for work purposes, including but not limited to generative AI assistants, AI writing tools, AI data analysis tools, and AI workflow automation systems.

The purpose of this policy is to enable productive and responsible AI adoption while protecting [Organisation Name], its clients, employees, and data from risks associated with AI misuse, data exposure, or unverified AI output.

2 Approved AI Tools

Only the following AI tools are approved for use in work contexts. Use of unapproved AI tools for work tasks is prohibited without prior written approval from [Policy Owner] .

APPROVED — ALL STAFF	APPROVED — SPECIFIC ROLES ONLY	NOT APPROVED
[e.g. Microsoft Copilot, Google Gemini, ChatGPT (paid)]	*[e.g. Claude for legal team, Perplexity for research leads]*	*[List any explicitly prohibited tools or categories]*

Employees who wish to use an unlisted AI tool must submit a request to [Policy Owner / IT Contact] for evaluation. Evaluation will assess data security, terms of service, and suitability for the intended use.

3 Acceptable & Prohibited Uses

✓ ACCEPTABLE USES

- Drafting, summarising, rewriting, and improving internal documents
- Research assistance for publicly available information
- Generating first drafts of proposals, reports, and communications
- Analysing data from approved internal systems

✗ PROHIBITED USES

- Entering client personal data, confidential contracts, or private financial information into public AI tools
- Using AI to make final decisions in HR, legal, medical, or financial matters without human review
- Representing AI output as the personal work or opinion of the employee
- Using AI tools not on the approved list for work purposes

- Automating repetitive, bounded, low-risk tasks with human review
- Learning and professional development activities

- Bypassing output review requirements for high-risk task categories

4 Data Privacy & Safe Sharing

Before entering any content into an AI tool, apply the following self-check:

1 Personal data?
Names, contacts, IDs, health, financial — do not enter into public AI tools

2 Client confidential?
Contracts, strategies, business information subject to NDA or confidentiality

3 Trade secrets?
Internal pricing, unreleased products, proprietary processes or formulas

4 Credentials?
Passwords, API keys, access tokens — never under any circumstances

If the answer to any of these questions is yes, do not enter the content into an external AI tool. Use only approved, internally hosted AI systems for such content, if available. When in doubt, contact [IT/Data Protection Contact] before proceeding.

Regulatory compliance: Use of AI tools must comply with all applicable data protection regulations, including [GDPR / CCPA / PIPEDA — select applicable]. Any suspected data breach involving an AI tool must be reported to [Data Protection Officer / IT Lead] within [24 / 48 / 72] hours.

5 Output Review & Verification Requirements

All AI-generated content used in a work context must be reviewed before use. The level of review required depends on how the output will be used.

RISK TIER	OUTPUT TYPE	REVIEW REQUIREMENT	WHO REVIEWS
Tier 1 Low	Internal drafts, brainstorming, personal notes, learning materials	Basic read-through. Employee verifies output is appropriate before using.	Individual employee
Tier 2 Medium	Client communications, proposals, published content, external reports	Fact-check all specific claims. Verify tone and accuracy. Have a colleague or supervisor review.	[Supervisor / Team Lead]
Tier 3 High	Legal documents, HR decisions, financial advice, medical information, regulatory filings	Full expert review by qualified professional required. AI output treated as research input only — not a final answer.	[Legal / HR / Finance Lead]

Employees may not represent AI-generated content as their own expert judgment. AI output must be verified before being attributed to an individual as professional advice, opinion, or certified fact.

6 Accountability & Escalation

Policy Owner: [Name / Role]
Responsible for maintaining, updating, and enforcing this policy. Reviews policy annually or when significant AI developments occur.

AI Tool Approval Authority: [Name / IT Lead]
Receives and evaluates requests to add new AI tools. Maintains the approved tool list.

Data Protection Contact: [Name / DPO]
First contact for questions about data privacy in AI use contexts.

ESCALATION PATH

1	Employee identifies an AI-related concern or incident
2	Reports to direct manager and documents the incident in writing
3	Manager notifies Policy Owner within [ ] business hours
4	Policy Owner assesses, involves legal/DPO if required, documents outcome

7 Training & Adoption Requirements

ALL STAFF
Must complete AI literacy training covering this policy, safe use practices, and output verification before using approved AI tools for work tasks.

TEAM LEADS & MANAGERS
Responsible for ensuring their teams are trained. Must understand Tier 2 review requirements and be capable of reviewing AI-assisted work for quality and compliance.

POLICY REVIEW CYCLE
This policy will be reviewed and updated *[quarterly / annually]* or whenever significant changes occur in approved tools, regulatory requirements, or organisational AI use.

8 Policy Breach & Consequences

Employees who violate this policy may be subject to disciplinary action, up to and including termination, depending on the severity and nature of the breach. This includes: using prohibited AI tools with client data, misrepresenting AI output as expert judgment, failing to apply required review levels, or knowingly bypassing governance controls.

Unintentional breaches should be reported promptly through the escalation path above. Good-faith reports will be treated with appropriate discretion.

POLICY SIGN-OFF & VERSION CONTROL

Policy Owner Signature	Approved by (CEO / HR Director)	Date of Approval

VERSION NUMBER	PREVIOUS VERSION DATE	KEY CHANGES IN THIS VERSION