INTAI

DOWNLOADABLE CHECKLIST

GOVERNANCE

AI Policy Readiness Checklist

Check whether your organisation's AI policies cover the practical rules, responsibilities, approved uses, prohibited uses and escalation routes employees need.

AI Policy Readiness Checklist

This checklist helps you assess whether your AI policy will actually guide real employee behaviour — covering scope, approved and prohibited uses, data rules, escalation routes and how the policy is communicated and kept current.

1 Coverage & Scope

Confirm the policy actually covers the ways AI is really being used across the organisation.

- ☐ **Does the policy cover generative AI tools used by staff, not only formally deployed AI systems?**
  Staff use of tools such as chatbots and writing assistants is often the largest, least visible source of AI risk.
- ☐ **Does the policy cover AI features embedded in existing software, not just standalone AI tools?**
  Many organisations are surprised to find AI already active inside tools they already use, without a formal procurement decision.
- ☐ **Is the policy applicable across all relevant functions, not written narrowly for a single department?**
  A policy written only with one team in mind often fails to anticipate how other functions actually use AI.
- ☐ **Does the policy apply to contractors and third parties working with organisational data, not only permanent staff?**
  Gaps here are a common, avoidable source of data exposure.

2 Approved & Prohibited Uses

- ☐ **Does the policy give concrete examples of approved AI use, not only abstract principles?**
  Concrete examples are far more useful to employees making day-to-day decisions than general statements of intent.
- ☐ **Does the policy clearly state which uses are prohibited, and why?**
  Prohibitions without a stated rationale are more likely to be quietly worked around.
- ☐ **Does the policy address use of AI with confidential, personal or commercially sensitive information?**
  This is one of the most common and highest-impact policy gaps, particularly regarding public generative AI tools.
- ☐ **Does the policy address AI-generated content requiring human review before external use?**
  Unreviewed AI-generated content reaching customers, regulators or the public is a recurring, avoidable incident type.

3 Roles & Responsibilities

- ☐ **Is it clear who employees should go to with questions about acceptable AI use?**
  A policy with no named contact point tends to be inconsistently applied or simply ignored under time pressure.

- ☐ **Is it clear who is responsible for approving new AI tools before they are adopted by a team?**
  Without a clear route, teams often adopt tools independently, outside any governance visibility.

- ☐ **Are manager responsibilities for enforcing the policy within their teams clearly stated?**
  Policies enforced only centrally, without manager engagement, tend to have inconsistent day-to-day adherence.

4 Data & Confidentiality Rules

- ☐ **Does the policy set clear rules on what data can and cannot be entered into external AI tools?**
  This is particularly important for smaller organisations relying heavily on consumer-facing AI products.

- ☐ **Does the policy reflect the organisation's obligations under GDPR regarding personal data?**
  Policy language should be specific enough to guide real decisions, not simply restate general GDPR principles.

- ☐ **Are there specific rules for particularly sensitive categories of data, such as special category data or safeguarding information?**
  Public sector bodies in particular often handle categories of data warranting stricter, explicit rules.

5 Escalation & Incident Reporting

- ☐ **Does the policy explain how to report a suspected AI-related incident or misuse?**
  A policy without a clear reporting route relies on individual judgement about when and how to raise concerns.

- ☐ **Is there a defined response process once an incident is reported?**
  Reporting without a defined response process undermines confidence in the reporting mechanism itself.

- ☐ **Does the policy make clear that reporting concerns in good faith will not be penalised?**
  Staff are considerably less likely to raise early warning signs if they fear the consequences of doing so.

6 Communication & Training

- ☐ **Has the policy been actively communicated to staff, rather than published and left for staff to find?**
  A policy that exists only on an intranet page is, in practice, rarely read or acted upon.

- ☐ **Is AI policy awareness included in onboarding for new staff?**
  Retrofitting awareness after someone has already formed their own habits is considerably harder than establishing it from day one.

☐ **Is there periodic refresher communication, given how quickly AI tools and associated risks change?**
A single training session at rollout is rarely sufficient on its own.

7 Review & Version Control

☐ **Is there a defined owner responsible for keeping the policy current?**
Without clear ownership, policies tend to drift out of date as AI use evolves.

☐ **Is there a scheduled review date, rather than an open-ended assumption that the policy remains adequate?**
Given the pace of change in this area, an annual review at minimum is appropriate for most organisations.

☐ **Is there a version history showing what has changed and when?**
This is useful both for internal governance and for demonstrating due diligence to regulators or auditors if required.

HOW TO SCORE THIS CHECKLIST

Pay particular attention to any 'No' answers in the Data & Confidentiality Rules and Escalation & Incident Reporting sections — these are the gaps most likely to result in a real incident before the wider policy is reviewed and strengthened.

INTAI

Need help acting on this checklist?

INTAI works with SMEs, public sector bodies and larger organisations across Europe to turn checklist findings into a practical, proportionate AI governance programme — from strategy and policy through to risk management and regulatory readiness. If you would like support closing the gaps this checklist has identified, our team is glad to help.

www.intai.co.uk | hello@intai.co.uk

© 2026 INTAI Limited. This checklist is provided for general guidance purposes only and does not constitute legal, regulatory or professional advice. Organisations should adapt it to their own context and seek independent advice where appropriate.