Responsible AI Policy Checklist

Key policy points for businesses using AI tools, from staff assistants to decision-support systems.

Nov 10, 2026 · @Vijay Srinivas Kothapalli

Purpose

AI tools are now inside everyday software: writing assistants, search, customer chat, accounting add-ons and recruitment screening. Many businesses use them without a written rule on what is allowed. This checklist gives a small or mid-sized business a short set of policy points to adopt, adapt and enforce.

It is written for owners, managers and the staff who choose or use AI tools, and for anyone who will be asked to approve an AI use later.

Scope

The policy covers any use of AI that touches your business, including:

- Generative tools that create text, images, code or summaries, used by staff in any function.
- AI features inside software you already buy, such as accounting, CRM, HR and customer support tools.
- Models your business builds, trains or fine-tunes, including those built on your own data.
- Automated tools that rank, score, screen or recommend people, customers or suppliers.

It does not replace your data protection, information security or employment policies. Where they overlap, the stricter rule applies.

Policy principles

Adopt these six principles as the foundation of every AI decision in the business:

1. **Accountability.** A named person is responsible for each AI use, including its outcomes.
2. **Purpose.** Each use has a clear business reason and a defined limit on what it may do.

3. **Data care.** Only the data needed for the purpose is used, and it is protected throughout.
4. **Human judgement.** People make the decisions that affect customers, employees and suppliers.
5. **Fairness.** Outputs are checked for unfair treatment before and during use.
6. **Openness.** People are told when AI has been used in a decision that affects them, and the business can explain how it reached that decision.

Checklist 1: Governance and ownership

- [ ] A named owner, usually a senior manager, is accountable for the AI policy.
- [ ] A list of approved AI tools is kept and reviewed each quarter.
- [ ] Each AI use in the business has a named business owner.
- [ ] The policy is approved by the owner or board, and reviewed at least once a year.
- [ ] Staff know whom to ask before adopting a new tool.

Checklist 2: Data handling

- [ ] Confidential, personal and financial data is not entered into an AI tool unless the tool is approved for that data.
- [ ] Free or personal accounts are not used for business data.
- [ ] The provider's terms confirm whether inputs are stored, used for training or shared with others.
- [ ] Customer and employee data used to build or test a model is lawful to use for that purpose and minimised.
- [ ] Outputs that contain personal data are handled under the same rules as the source data.
- [ ] Access to AI tools and their stored history is limited to people who need it.

Checklist 3: Human review and decisions

- [ ] AI may draft, summarise or suggest. A person reviews and approves anything sent to a customer, supplier or regulator.
- [ ] Decisions on hiring, dismissal, credit, pricing for individuals, or access to services are never made by AI alone.

- [ ] Staff are trained to check AI output for errors, invented facts and missing context.
- [ ] The reviewer has the authority and time to reject an output.
- [ ] Records show who reviewed an output where it affects a person or a payment.

Checklist 4: Fairness and customer impact

- [ ] Before use, the AI tool is tested on realistic cases, including the groups it could affect unfairly.
- [ ] Screening or scoring tools are checked for different results across groups, and the results are recorded.
- [ ] Customers are told when an automated tool has played a material part in a decision about them, and how to ask for a human review.
- [ ] Complaints about AI-assisted decisions are logged and reviewed.
- [ ] Pricing or offers are not varied by AI in ways that treat similar customers unfairly.

Checklist 5: Vendors and third-party AI

- [ ] Every AI feature inside a supplier's product is listed, not only the tools you chose on purpose.
- [ ] Contracts state how the supplier uses your data, where it is processed and whether it is used to train models.
- [ ] Suppliers must tell you about material changes to their AI models or their subcontractors.
- [ ] You can switch off an AI feature without losing access to the core service.
- [ ] Suppliers provide information on testing, limitations and known failure modes when asked.

Checklist 6: Transparency and records

- [ ] A register lists each AI use, its owner, its purpose, the data it uses and its risk level.
- [ ] Significant decisions made with AI assistance are recorded with the reviewer's name and date.
- [ ] Staff and customers can find out, in plain words, where AI is used in the business.
- [ ] Logs of prompts, outputs and changes are kept for the period your obligations require.

- [ ] The business can explain, in plain words, why an automated output led to a particular decision.

Acceptable use rules for staff

Post these rules where staff can see them, and include them in induction.

Allowed, with care

- Drafting routine emails, summaries and first versions of documents, which are then checked by the author.
- Brainstorming, translating general text and explaining concepts.
- Using approved tools for internal work that contains no confidential or personal data.

Not allowed

- Pasting customer records, employee files, passwords, bank details, unreleased financials or contracts into any tool that is not approved.
- Using AI to make a final decision about a person without human review.
- Presenting AI output as verified fact without checking it.
- Installing AI browser extensions or add-ons without approval.

When in doubt, ask the named owner before using the tool.

Assessing a new AI use before it goes live

Use this short assessment for any new tool or use case. A simple use can be approved in a day. A use that affects customers or employees needs the full review.

1. **Describe the use.** What will it do, for whom, and what decision or output will it produce?
2. **Identify the data.** What data goes in, what comes out, and where is each one stored?
3. **Check the supplier.** Read the terms, the data location, and whether inputs train the model.
4. **Test it.** Run realistic examples, including unusual or sensitive cases, and record the errors.
5. **Set the human check.** Decide who reviews outputs and what they must check.
6. **Assess the impact.** Could it treat any group or person unfairly, or cause financial or reputational harm?

7. **Approve or refuse.** The business owner signs off with the conditions written down, and the use goes into the register.

Monitoring, incidents and review

AI tools change often. Review each approved use at least once a year, and sooner if the tool, its terms or the use changes.

Treat these as incidents and log them:

- An output that exposed personal or confidential data.
- A wrong or invented output that was acted on.
- A complaint from a customer or employee about an AI-assisted decision.
- A supplier announcing a material change to its AI model or data handling.

For each incident, record what happened, who was affected, what was done, and what will prevent a repeat. Report material incidents to the owner the same day.

Adopting the policy in 90 days

Period	Action	Owner
Days 1 to 30	List every AI tool in use, including those inside existing software.	Operations or IT lead
Days 1 to 30	Name the policy owner and approve the principles.	Owner or board
Days 31 to 60	Classify each use by data sensitivity and impact. Stop any use that breaks the data rules.	Business owners
Days 31 to 60	Review supplier terms for training use and data location.	Finance or legal adviser
Days 61 to 90	Issue the staff rules and run a short training session.	Owner and HR lead
Days 61 to 90	Start the AI register and set the first annual review date.	Owner

By day 90, every AI use should have a named owner, a documented review and a clear rule for staff.

About CRCO LLP

CRCO LLP is a Hyderabad-based advisory firm working with businesses on cybersecurity, data privacy and protection, outsourcing, process improvement and automation. We help businesses adopt AI with clear ownership, sensible data rules and reviews that work in practice.

Book a consultation: visit the Contact page on our website, or write to us through the enquiry form.

This checklist provides general guidance only. It is not legal advice. Obligations on data use and automated decisions depend on your sector and circumstances, and should be confirmed with a qualified adviser.