

AI Ethics Training Rollout Checklist

From AI-use assessment to post-training reinforcement: practical questions, ownership cues, red flags, and next steps.

Assess

Design

Launch

Reinforce

Measure

#1 Establish the baseline

Question to answer	Who should contribute
Which AI tools are employees actually using?	IT + security + business teams
Which uses are officially approved?	IT/security + legal/compliance
Which AI uses affect customers, employees, or other high-impact decisions?	Business owners + legal/compliance
What data goes into these systems?	IT/security + process owners
Where are employees already making mistakes or asking questions?	Managers + IT/security + HR/L&D
Which regulations and industry requirements apply?	Legal/compliance + relevant SMEs
Which roles need more than the shared foundation?	HR/L&D + business leaders

#2 Decide what employees should be able to do

Tailor to company specifics



"Employees understand responsible AI."

- ☐ Identify information that must not be entered into an AI tool?
- ☐ Distinguish approved from unapproved tools?
- ☐ Recognize when an AI output requires verification?
- ☐ Identify a potentially discriminatory or unsafe outcome?
- ☐ Know when human review is mandatory?
- ☐ Know where to report an uncertain use case?

blue carrot

#3 Build the learning architecture

Specialization <i>(do you need separate learning paths?)</i>	Maturity <i>(how much content for each path is needed?)</i>	Risk <i>(how intensive does the training need to be?)</i>
Would employees choose differently in similar situations?	Do they understand its basic limitations and common risks?	Could a mistake harm a person or customer?
Do groups use AI for different types of work?	Do employees already use AI regularly?	Does AI influence a high-impact or consequential decision?
Do those uses involve different rules, risks, or decisions?	Do they understand its basic limitations and common risks?	Could it have privacy, security, legal, or financial risks?
One shared course, dedicated modules, or separate role-specific learning paths	Foundation + guided practice, real-world application, or edge cases	Awareness + simple scenarios, practice + reinforcement, or extensive scenarios

#4 Translate rules into scenarios

Situation	What happened?
Decision	What does the employee have to decide?
Options	What could they realistically do?
Feedback	Why is one choice preferable?
Escalation	What happens if the answer isn't obvious?

#5 Check the learning experience before launch

⊘ Stop and fix	⚠ Review	✓ Ready
Course contradicts policy.	Some scenarios are hypothetical.	Scenarios reflect actual workflows.
Employees are told to use tools they cannot access.	Certain roles receive identical content despite different risks.	Feedback explains reasoning.
There is no escalation route. Unclear who owns AI-related questions.	Assessment mainly tests recall.	Learners practice rather than only read.
Employees assessed on rules they have never been taught.	Training is long enough that completion may become a problem.	Role-specific risks are represented.
		Policies and approved tools match the course.

#6 Make corrections post-launch

 Employees repeatedly fail the same scenario? ➤ Check whether the scenario is unrealistic. ➤ Review the relevant content. ➤ Test the revised version with a small group.	 Employees report many ambiguous cases? ➤ Potentially a policy gap. ➤ Escalate to the relevant policy owner and update guidance.
 Employees complain about the training? ➤ Separate "inconvenient" from "irrelevant." ➤ Check workload, length, format, relevance, and manager support.	 Employees pass but ignore the rule? ➤ Check the workflow, incentives, tool availability, and manager behavior. ➤ Don't automatically add another training module.
 A regulation or policy changes? ➤ Identify affected roles and scenarios to update. ➤ Trigger targeted refreshers instead of retraining everyone.	 New learner feedback reveals a gap? ➤ Identify the root cause. ➤ Update the relevant content or practice. ➤ Test the change before rolling it out broadly.

#1 Establish the baseline

 Activity	 Primary owner	 Also consult
AI-use inventory	AI program owner / IT	Business teams
Risk identification	Legal/compliance / security	Process owners
Learning objectives	L&D	SMEs + managers
Regulatory validation	Legal/compliance	SMEs
Course design	L&D / learning partner	SMEs
Technical implementation	IT/LMS owner	L&D
Employee communications	HR/comms	Managers