



Ennis Studio

FREE CHECKLIST · 30 QUESTIONS · ABOUT 30 MINUTES

The Shadow AI and AI Use Policy Checklist

Find the AI already running in your business and see what your policy needs to cover.

START HERE

How to use this checklist

Work through it with whoever runs IT (in-house or your managed service provider) and one operations leader. Mark each item:

Yes Done, written down, and you can show it.	Partly Informal, out of date, or true for some teams only.	No Not in place, or you don't know.
--	--	---

"I don't know" counts as **No**. Finding out is the point. At the end, count your No answers in each section and use the scoring guide.

SECTION 1

Find the AI you already have

You can't set rules for tools you can't see.

#	QUESTION	YES	PARTLY	NO
1	We have asked staff, anonymously, which AI tools they use for work, including on personal phones and accounts.	☐	☐	☐
2	We have a written list of every AI tool in use: chat assistants, writing tools, meeting note-takers, browser extensions, and AI features inside software we already pay for.	☐	☐	☐
3	We have checked our main business software (ERP, CRM, email, office suite, accounting) for AI features that were switched on in recent updates.	☐	☐	☐
4	We know which meeting note-takers or recording bots join our calls, including bots invited by customers and vendors.	☐	☐	☐
5	We have reviewed which apps staff have connected to company email, calendars or file storage with "Sign in with Microsoft/Google."	☐	☐	☐
6	We know whether anyone has built their own automation, agent or custom GPT that touches company systems or data, and who owns it.	☐	☐	☐

Quick tip: Ask the survey question as "What AI tools help you get work done?", not "Are you breaking the rules?" You'll get far more honest answers.

No answers in this section: _____

SECTION 2

Know your data

The rules depend on what's being pasted in.

#	QUESTION	YES	PARTLY	NO
7	We have named the three to five types of data we'd most hate to see leaked (for example customer drawings, pricing, payroll, supplier contracts, health information).	☐	☐	☐
8	Our data is sorted into simple classes such as Public, Internal, Confidential and Restricted, and staff know what goes in each.	☐	☐	☐
9	We know which data we hold under customer contracts, NDAs or supplier agreements that limit where it can go.	☐	☐	☐
10	We know which data is regulated for us (for example employee records, payment card data, health information, export-controlled technical data).	☐	☐	☐
11	We have checked whether any customer contract forbids putting their data into third-party AI tools.	☐	☐	☐

No answers in this section: _____

SECTION 3

Check the tools you pay for

A business account helps only if it's set up right.

#	QUESTION	YES	PARTLY	NO
12	For each approved AI tool, we have read its business data terms and know whether our inputs are used to train its models.	☐	☐	☐
13	Model training on our data is switched off wherever the vendor offers that setting.	☐	☐	☐
14	Staff sign into AI tools with company accounts (single sign-on where possible), not personal email addresses.	☐	☐	☐
15	We know how long each tool keeps prompts, uploaded files and chat history, and whether we can delete them.	☐	☐	☐
16	Admins can see usage and can remove a user's access the day they leave.	☐	☐	☐
17	AI tools that can read company files only see what that user is already allowed to see. Access in file storage has been reviewed recently.	☐	☐	☐

Quick tip: AI assistants that search your company files are only as safe as your file permissions. If "Everyone" can open the payroll folder, the assistant can summarize it for anyone who asks.

No answers in this section: _____

SECTION 4

Write the rules

The policy people will actually read.

#	QUESTION	YES	PARTLY	NO
18	We have a written AI acceptable-use policy that leadership has approved.	☐	☐	☐
19	The policy lists approved tools by name, plus a simple way to request a new one.	☐	☐	☐
20	It states plainly which data classes can and cannot go into which tools.	☐	☐	☐
21	It requires a person to review AI output before it reaches a customer, goes into a quote or contract, or affects a hiring or employment decision.	☐	☐	☐
22	It covers AI-generated content we publish or send: accuracy, disclosure where required, and who signs off.	☐	☐	☐
23	It covers staff building their own automations or agents: who approves them, what they can connect to, and who owns them.	☐	☐	☐
24	There is a one-page plain-language version for staff, not just a long policy document.	☐	☐	☐

No answers in this section: _____

SECTION 5

Make it stick

A policy nobody follows is just a document.

#	QUESTION	YES	PARTLY	NO
25	One named person owns AI decisions and keeps the approved-tools list current.	☐	☐	☐
26	New hires learn the AI rules during onboarding, and current staff have been walked through them.	☐	☐	☐
27	Staff know who to tell, and how quickly, if they paste something they shouldn't have, and they know they won't be punished for reporting it.	☐	☐	☐
28	Our incident response plan covers AI-related data exposure.	☐	☐	☐
29	New AI tools go through a short security and data review before purchase, including AI features added to software we already own.	☐	☐	☐
30	We review the policy and tools list at least twice a year.	☐	☐	☐

No answers in this section: _____

RESULTS

Scoring guide

Count your No answers in each section.

SECTION	0 NO	1-2 NO	3+ NO
1. Find the AI	You have good visibility	Blind spots likely	You don't know what's running
2. Know your data	Ready to write rules	Classify before you write rules	Start here
3. Check the tools	Accounts set up well	Settings need attention	Exposure likely today
4. Write the rules	Policy in place	Gaps to close	No real policy yet
5. Make it stick	Well governed	Needs an owner and a rhythm	Policy won't hold

10 or more No answers in total? You're in the majority. Only 23% of U.S. businesses with 5-499 employees have a documented AI use policy ([Pax8](#), [SMB AI Report Q2 2026](#)). The fix takes days, not months.

Five things you can do this week

1. **Send the anonymous survey.** Ask one question: "Which AI tools help you get work done, and what do you use them for?"
2. **Turn off model training** on every business AI account you already pay for.
3. **Name your "never paste" list.** Three to five data types, shared with every employee by email today.
4. **Pick one owner.** One person decides which tools are approved.
5. **Review file permissions** before you switch on any AI assistant that searches company files.

SAFE AI ADOPTION WORKSHOP

Want it done in one session?

The workshop turns this checklist into four finished documents in one 3-hour session: an AI acceptable-use policy, an approved-tools list with risk ratings, data-handling rules, and a one-page staff guide.

\$3,000 FIXED FEE · DELIVERED WITHIN 5 BUSINESS DAYS · REMOTE OR ON-SITE IN WEST MICHIGAN

ennis-studio.com/for/operations/safe-ai · [Book a 20-minute fit call](#) · [See a sample deliverable](#)

This checklist is general operational guidance, not legal advice. Have counsel review any policy before you adopt it, especially if you handle regulated data. © 2026 Ennis Studio.