

AI Privacy Checklist

10 habits for safer AI use

10 practical habits for small business teams in 2026

Print or share this page. Assign an owner and a monthly review date. These habits reduce risk; they do not replace judgment.

1

Use the right account

Use the approved business workspace or account for client and company work; keep personal accounts out of client data.



2

Review training controls

Know whether new chats can be used to improve the provider's models and turn training off where the tool allows.



3

Think before giving feedback

Feedback submissions can include the full conversation; do not submit sensitive threads without reviewing the policy.



4

Treat shared links as sharing

Review the entire chat and any attachments before creating a share link; assume anyone with the URL can read it.



5

Use temporary modes appropriately

Non-persistent modes are useful for one-off work but are not permission to disclose passwords, keys or restricted data.



6

Understand memory

Some tools carry context across chats. Treat memory and model-training controls as separate settings.



7

Audit old shared links

Revoke shared links that no longer need to exist; add this to a quarterly review, not a one-time task.



8

Check feature-specific controls

Coding tools, agents, browsers and other capabilities can have their own privacy settings distinct from chat.



9

Review apps and extensions

Only connect trusted services and remove integrations you no longer use; each connector expands the trust boundary.



10

Protect real secrets

Keep passwords, API keys, tokens, PHI, PII and other restricted data out of casual prompts.



AI Privacy Checklist

Questions and governance

Before you paste: 7 questions to ask

Run through this list any time a prompt is going to include client, employee or business information.

- ☐ Am I authorized to share this information with this provider?
- ☐ Am I using the approved business account or workspace?
- ☐ Do I understand the training, retention and sharing settings for this tool?
- ☐ Does the AI actually need this sensitive detail to complete the task?
- ☐ Can I replace it with a placeholder, redaction or summary?
- ☐ Have I reviewed attachments for unnecessary sensitive information?
- ☐ Am I about to create a share link or send feedback for this thread?

Small business AI governance: your rules

Fill in each row with your policy. Post it where the team can see it and review quarterly.

Decision	Your rule
Approved AI tools	Which providers are on the approved list.
Approved account / workspace	Which login staff must use for company work.
Prohibited data	What must never be pasted into any prompt.
Restricted data requiring approval	What can be used with a sign-off.
Approved apps / extensions	Which connectors are allowed.
Who can approve exceptions	Named decision-maker for edge cases.
Shared-link review cadence	How often shared links are audited.
Employee training cadence	How often the team reviews the policy.

Privacy settings reduce risk. They do not replace judgment.

Share only what is necessary for the task. When in doubt, ask before you paste.