AI DATA-SAFETY CHECKLIST

What Small Businesses Should Never Paste Into AI Tools

Simple boundaries for using AI without casually exposing customer, financial, confidential, or business-sensitive information.

Kishor Nair

AI Automation & Digital Marketing



START HERE

Before your team uses AI, create a never-upload list.

AI can save a small business hours of work, but convenience can make it easy to paste information into a tool without considering whether that information should leave its original system.

The goal is not to avoid AI. Decide what is appropriate to use, what needs protection or approval, and what should stay out of general-purpose AI tools entirely.

THE SIMPLE RULE

If the information would cause a customer, employee, partner, or your business harm if it were exposed, do not paste it casually into an AI tool.

Use three zones

NEVER PASTE

Secrets, credentials, highly sensitive personal data, or information you are not authorized to share.

PAUSE & CHECK

Confidential business or customer information that may be usable only with approval, redaction, or an approved tool.

GENERALLY SAFER

Public, synthetic, anonymized, or non-sensitive information - while still checking your company's rules and the tool's settings.

RED ZONE

What should never be pasted casually

Treat these categories as a default stop sign unless your organization has explicitly approved the specific tool and use case.

Passwords & credentials

Passwords, PINs, API keys, private keys, authentication tokens, recovery codes, access links, or security answers.

Payment & banking details

Full card details, CVV, bank login credentials, payment credentials, or information that could enable unauthorized transactions.

Highly sensitive personal information

Government ID numbers, passport details, medical information, biometrics, or similarly sensitive records unless there is a specifically approved and compliant workflow.

Customer records

Raw customer databases, contact lists, account histories, support records, or files containing identifiable customer information without a valid approved reason.

Employee confidential information

Payroll details, disciplinary records, performance issues, identity documents, health information, or private HR records.

Confidential legal or contractual material

Privileged legal advice, confidential settlement discussions, unreleased contracts, or restricted documents unless approved for that system.

AMBER ZONE

Pause before sharing business-sensitive information

Some information may be useful for AI-assisted work, but that does not mean it should be pasted into any AI tool. Check sensitivity, authorization, the tool, its settings, and the purpose first.

☐ Unpublished pricing, margins, forecasts, budgets, or financial reports

☐ Internal strategy, acquisition plans, product roadmaps, or board material

☐ Customer emails, call transcripts, proposals, contracts, or support conversations

☐ Employee names, CVs, evaluations, compensation, or internal communications

☐ Supplier terms, partner agreements, negotiated rates, or confidential quotations

☐ Source code, proprietary processes, internal documentation, or trade secrets

☐ Unreleased marketing plans, campaign data, research, or competitive intelligence

ASK BEFORE YOU PASTE

Do I need the real data for this task? If not, remove names, identifiers, account details, confidential numbers, and unnecessary context. Use placeholders or synthetic examples instead.

SAFER WORKING

Give AI the minimum information it needs

Good AI use is often about reducing the amount of sensitive context you share, not simply deciding between 'use AI' and 'don't use AI'.

1. REDACT

Remove names, email addresses, phone numbers, IDs, account numbers, confidential figures, and other identifiers.

2. REPLACE

Use placeholders such as [CUSTOMER], [COMPANY], [PRICE], [LOCATION], or [ACCOUNT TYPE].

3. SUMMARIZE

Describe the situation instead of uploading the original email, contract, spreadsheet, or customer record.

4. SYNTHESIZE

Create fictional sample data that preserves the structure of the problem without exposing real people or business information.

5. MINIMIZE

Share only the fields or excerpt actually required for the task.

6. USE APPROVED SYSTEMS

Use tools and configurations your business has reviewed for access, retention, training, security, and contractual requirements.

10-SECOND CHECK

Before pasting anything into AI

Use this checklist whenever material comes from a customer, employee, internal system, partner, or confidential document.

☐ Is this information public, or am I authorized to share it with this AI system?

☐ Does it contain a password, credential, API key, token, or security information?

☐ Does it identify a customer, employee, prospect, patient, student, or other individual?

☐ Does the AI actually need the person's identity to complete the task?

☐ Does it contain financial, legal, health, HR, contractual, or commercially sensitive information?

☐ Can I redact, summarize, anonymize, or replace the real data with placeholders?

☐ Do I know how this AI tool handles data, retention, access, and model training for my account or plan?

☐ Has my business approved this tool for this type of information?

☐ Would I be comfortable explaining this upload to the customer or data owner?

☐ If I am unsure, can I stop and ask the responsible person before sharing it?

IF YOU ARE UNSURE

Do not paste first and investigate later. Remove the sensitive information, use a fictional example, or confirm your business's policy and the tool's data controls.

TEAM POLICY

A one-page AI data-safety rule for your business

Print this page or adapt it into your internal AI-use policy.

1 — NEVER SHARE

Passwords, authentication secrets, payment credentials, highly sensitive personal records, or information we are not authorized to disclose.

2 — MINIMIZE BY DEFAULT

Remove names, identifiers, confidential numbers, and unnecessary context. Use placeholders, summaries, or synthetic examples whenever possible.

3 — USE APPROVED TOOLS

Business information should only be used with AI systems and account settings that the business has approved for that category of data.

4 — KEEP HUMAN RESPONSIBILITY

AI output does not remove our responsibility for privacy, confidentiality, accuracy, customer commitments, or final decisions.

Team acknowledgement

Name: _____ Date: _____

Signature: _____

FINAL CHECK

Use AI confidently — with clear boundaries.

Small businesses do not need a complicated rulebook before using AI. They do need a shared understanding of what information should never be casually uploaded, when to pause, and how to reduce unnecessary exposure.

> **REMEMBER**
>
> AI can assist the work. Your business remains responsible for the data.

Your next three actions

☐ Create a written never-upload list for your team.

☐ Choose which AI tools are approved for business use and review their current data controls.

☐ Teach everyone to redact, minimize, and use placeholders before sharing business information.

Kishor Nair

AI Automation & Digital Marketing

Practical AI adoption for small businesses — with human judgment, sensible controls, and clear accountability.

Important: This checklist is general educational guidance, not legal, privacy, cybersecurity, or regulatory advice. Requirements vary by business, location, industry, data type, contracts, and the AI service being used.