VIRTUOUS BIZNIZ LLC

The Green-Amber-Red
AI Data Classification Guide

What goes into AI tools. What doesn't. And the 3-second rule that protects you.

Free resource from Virtuous Bizniz LLC — virtuousbizniz.com

This guide gives you a practical, printable framework for classifying your data before using any AI tool. It takes 3 seconds to apply. It prevents the majority of AI data incidents.

HOW TO USE THIS GUIDE

Before you input anything into a public AI tool (ChatGPT, Claude, Gamma, Fireflies, or any other), ask yourself: is this Green, Amber, or Red? Print this page and keep it next to your screen. Share it with your team.

GREEN — APPROVED

Safe to use in any AI tool, any time, without restriction.

Green data contains no proprietary, personal, or confidential information.

- ✓ Public research and information available online or in published sources
- ✓ Generic templates using fictional companies, hypothetical scenarios, or placeholder names
- ✓ Brainstorming and ideation with no client or company-specific context
- ✓ General writing tasks: blog posts, social media, newsletters using no internal data
- ✓ Code for non-proprietary, non-client applications using generic variable names
- ✓ Training material frameworks using hypothetical examples (no real client scenarios)
- ✓ Publicly available statistics, research, and industry reports
- ✓ Interview question frameworks with no company-identifying content

AMBER — CONDITIONAL

Safe to use in AI tools only after removing identifying information.

The CONDITION for every Amber item: remove company names, client names, employee names, deal values, and any specific identifying details before inputting.

Internal strategy documents	*Condition: Remove company name, client names, financial projections, and any market-sensitive details*

HR policy templates	*Condition: Use generic job titles and department names. No employee names, salary figures, or performance data*
Process documentation	*Condition: Describe the process structure — not the specific client, project, or system names*
Meeting notes and summaries	*Condition: Remove participant names, client names, deal values, and any confidential decisions before inputting*
Training materials based on real scenarios	*Condition: Replace all real names and company references with fictional equivalents*
Proposal structures	*Condition: Use the structure and section headings — not client names, pricing, or proprietary methodology details*
Internal communications	*Condition: Remove names, roles, and any company-identifying context*

RED — PROHIBITED

Never input into any public AI tool. No exceptions. No "just this once."

Red data is any information that could cause legal, financial, reputational, or personal harm if accessed by a third party — which a public AI tool is.

- ✗ Customer or client personally identifiable information (PII) — names, emails, phone numbers, addresses, ID numbers
- ✗ Financial records — revenue, profit, pipeline values, deal amounts, payment history, bank details
- ✗ CRM data of any kind — Salesforce records, HubSpot contacts, pipeline data, account information
- ✗ Employee HR files — performance reviews, salary data, disciplinary records, personal information
- ✗ Confidential contracts — client agreements, supplier contracts, partnership terms, NDAs
- ✗ Legal documents — case files, privileged communications, settlement details
- ✗ Medical or health records — patient data, treatment information, insurance details
- ✗ Any information covered by a non-disclosure agreement or confidentiality clause
- ✗ Unpublished intellectual property — unreleased products, proprietary methods, trade secrets
- ✗ Authentication credentials — passwords, API keys, security tokens, access codes

The 3-Second Rule

Before anything goes into a public AI tool — ask yourself one question:

"Is this Green, Amber, or Red?"

3 seconds. Every time. This single habit prevents the majority of AI data incidents.

The Salesforce Exception

For Salesforce professionals: Einstein AI tools (Copilot, Flow AI, Prompt Builder) operate inside the Salesforce Trust Layer. Data never leaves your Salesforce environment. These tools are effectively Green — safe for all client data.

All other AI tools — ChatGPT, Claude, Gamma, Canva AI, Fireflies, etc. — are public AI tools. The Green-Amber-Red framework applies to everything you input into them.

The Enterprise Exception

Enterprise versions of AI tools (ChatGPT Enterprise, Claude for Business, Microsoft Copilot in M365) operate under Data Processing Agreements (DPAs). Data is not used to train models and is subject to your jurisdiction's data handling requirements.

For organisations that regularly handle Amber-tier data and need AI assistance, upgrading to enterprise tools is the compliant path. The cost is higher than consumer tools — and significantly lower than the cost of a compliance breach.

WANT THE FULL AI GOVERNANCE POLICY TEMPLATE?

The Green-Amber-Red framework is Section 2 of the Virtuous Bizniz AI Governance Policy Template. The full 6-section policy — customisable for your organisation — is available as part of the AI Security Sprint engagement. Email ohi@virtuousbizniz.com to learn more.

SHARE THIS GUIDE

This guide is free to share with your team. Print it. Post it. Send it. The more people who know these rules, the fewer organisations get hurt by preventable AI incidents.