

1 AI A DAY · @JJWONG.AI

The Safe-Paste Pack

1 AI A Day · Day 14 · @jjwong.ai

JJ Wong · jjwong.ai

The anonymiser that strips personal data in one pass, and a one-page AI policy short enough that your team will actually read it.

The five things that never go in

NEVER PASTE	BECAUSE
Customer personal data — names, phones, addresses, IC numbers	It isn't yours to hand to a third party
Payment details — card numbers, bank accounts, statements	Same reason, with worse consequences
Credentials — passwords, API keys, tokens, recovery codes	Once it's in someone's chat history, treat it as leaked. Rotate it.
Third-party contracts	Many contracts restrict sharing their terms
Anything under NDA	A client's data isn't yours to share, with anyone

None of this is about whether you trust the AI company. It's about what you're allowed to give any third party at all.

The rule that covers most of it

Strip first. Always. Never case by case.

Nearly every task still works with identifiers removed. You want to know what customers keep asking — you don't need their names for that. You want a reply drafted — the phone number adds nothing. The moment anonymising becomes a judgement call ("this one's probably fine"), something slips through.

The anonymiser

Run these in this order. They catch the common Malaysian formats.

ORDER	REPLACES	PATTERN	WITH
1	Emails	<code>[w.+-]+@[w-]+\.[w.-]+</code>	<code>[EMAIL]</code>
2	MyKad numbers	<code>\b\d{6}-?\d{2}-?\d{4}\b</code>	<code>[IC]</code>
3	Malaysian mobiles	<code>(\+?6?0)1\d[\s-]?\d{3,4}[\s-]?\d{4}</code>	<code>[PHONE]</code>
4	Order-ID-like strings	<code>\b[0-9A-Z]{10,}\b</code>	<code>[ORDER]</code>

In Google Sheets, text in column A, all four at once:

```
=REGEXREPLACE(REGEXREPLACE(REGEXREPLACE(REGEXREPLACE(A2,
"\w.+-]+@[w-]+\.[w.-]+","[EMAIL]"),
"\b\d{6}-?\d{2}-?\d{4}\b","[IC]"),
"(\+?6?0)1\d[\s-]?\d{3,4}[\s-]?\d{4}","[PHONE]"),
"\b[0-9A-Z]{10,}\b","[ORDER]"))
```

Fill down, copy, paste as values over the original, delete the raw column.

Three things patterns can't do:

- **Names.** Replace the whole username or buyer column with `[BUYER]`.
- **Addresses.** Delete the column. You almost never need it for AI work.
- **Creative formats.** "zero one two, three four five..." won't be caught by anything. Spot-check ten rows by eye every time.

Rule 4 will also catch long all-caps SKU codes. If your SKUs look like order IDs, adjust the `{10,}` to your platform's order ID length, or skip that rule.

The real risk: personal accounts

If your team uses AI at work, some of them are pasting work data into free personal accounts. Consumer tiers of AI tools often allow the provider to use what you submit to improve their models; business and team tiers usually don't by default. Check the data-use terms for the specific tool and plan you use — they differ, and they change.

A policy that says "don't paste customer data" means little if the only tool your team has is a personal login. Giving them a proper business account costs less than one incident.

Check once a quarter: which tools the team actually uses, what plan each is on, and what that plan's data settings are.

The one-page team policy

Copy this, change the bracketed parts, and pin it wherever your team works.

HOW WE USE AI AT [BUSINESS NAME]

Use: [approved tool(s)] on the company account only.

Not: personal accounts, free tiers, or tools not on this list.

Never paste:

1. Customer names, phone numbers, addresses, IC numbers
2. Card, bank or payment details
3. Passwords, API keys, tokens or login codes
4. Contracts or documents from suppliers or clients
5. Anything a client told us is confidential

Always:

- Run the anonymiser before pasting any chat log, order list or export.
- Check any number, fee, policy or rule the AI gives you before acting on it.
- Read every customer-facing reply before it's sent. AI drafts, a person sends.

If you're not sure whether something is OK to paste — it isn't. Ask [name].

If you think something was pasted that shouldn't have been, tell [name] straight away. Nobody gets in trouble for reporting it. Credentials get rotated.

Last reviewed: [date]

Short on purpose. A policy nobody reads is a policy that doesn't exist.

The question to ask before every paste

"Would I be comfortable if this exact text showed up in a screenshot someone else shared?"

If not, strip it or don't paste it. That one question catches nearly everything on this page.

Questions? Reply to this email — I read them all. More at @jjwong.ai — one AI play for SEA sellers, daily.