PDPA PROGRAMME PACK · B14

Basic AI-use policy

Fictional organisation, illustrative only, not a client case study. Quillmarrow Supplies Pte. Ltd. (fictional) is invented. All people are shown by role only.

Organisation	Quillmarrow Supplies Pte. Ltd. (fictional)
Document	B14 · Basic AI-use policy
Version	1.0
Date	30 October 2026 (illustrative)
Prepared by	Alex Lew, reviewer and sign-off
Client approver (role)	Managing Director
Label	Fictional organisation, illustrative only, not a client case study

1. Why Quillmarrow needs this now

About 80 Quillmarrow staff already use Microsoft 365 Copilot, and some use ChatGPT, to draft emails, summarise documents and write product copy. The PDPA programme found no written rule on what may go into these tools. The risk is practical: a helpdesk transcript (PD-06), a CV (PD-15) or a returns spreadsheet like the one in INC-2026-07 pasted into the wrong tool is a disclosure Quillmarrow cannot take back.

This one-page policy sets the minimum rules until the separate AI governance review (the batch A pack) is approved. Where the two differ, the AI governance pack wins once the MD signs it.

Scope: all staff, contractors and Fictional Harbour IT staff working on Quillmarrow systems, on company or personal devices, whenever Quillmarrow information is involved.

Owner: COO. **Approver:** Managing Director. **Questions:** the IT Manager for tools, the Head of Operations as appointed DPO for personal data. **Status:** draft v1.0 for MD approval.

Words used here. *AI tool* means any service that generates or summarises text, images or code, including features built into other software. *Personal data* means data about an identifiable person, as listed in the B3 inventory. *Approved* means listed by the IT Manager under section 2.

2. Which tools, for what

Tool	Allowed for	Not allowed for
Microsoft 365 Copilot (company licence)	Drafting and summarising internal documents you already have access to; meeting notes; first drafts of customer replies that you then check.	Anything involving PD-15 job applications, PD-18 medical records or PD-19 NRIC/FIN copies; decisions about a person.
AI features inside approved vendor tools (for example Fictional Helpdesk reply suggestions)	Only where the IT Manager has listed the feature as switched on and reviewed under B9.	Any feature you switch on yourself.
Personal ChatGPT or other personal AI accounts	General questions with no Quillmarrow information, such as grammar or a public topic.	Any customer, staff or supplier data, contract terms, prices not yet published, or internal files.

If a tool is not on this list, ask the IT Manager before using it for work.

3. Never put these into any AI tool

- NRIC or FIN numbers, or copies of identity documents (PD-19).

- Payment details of any kind, even partial (PD-03).
- CVs, application forms or interview notes (PD-15).
- Medical certificates or leave reasons (PD-18).
- Whole exports or spreadsheets of customers, B2B contacts or prospects (PD-01, PD-04, PD-10).
- Confidential contract terms, including the DV-01 Malaysia logistics contract.

Taking a name out does not make a record anonymous. An address, order number and product together can still identify a customer. If you need an example, make one up.

4. Check every output before it leaves you

AI output can be confident and wrong. Before you send or publish it, check:

1. **Facts and product claims** against the approved product sheet. Remove anything you cannot support.
2. **Prices and stock** against Fictional StockPoint and the approved price list, never the AI's figure.
3. **Personal data** that should not be there, such as another customer's details in a drafted reply.
4. **Promises.** Customer Service replies must not promise refunds, deadlines or outcomes that the process does not allow.

5. People decide about people

AI must not decide anything about a customer, applicant, employee or supplier on its own: not a hiring shortlist, a credit application (PD-05), a complaint outcome or a disciplinary matter. A named staff member reviews the facts and makes the decision through the normal process. Under this policy, CVs do not go into AI tools at all, so AI-assisted shortlisting is not allowed until the AI governance pack approves it.

6. If something goes wrong

If you paste personal data into the wrong tool, or send an AI-drafted message to the wrong person, tell the DPO and the IT Manager **the same day**. Say which tool, what data, roughly how many people and when. Do not delete the evidence or try to fix it quietly.

The DPO then follows **B11**. The DPO assesses the facts first: whether the incident is likely to cause significant harm, or affects 500 or more people. The MD and DPO then decide, as a separate recorded step, whether to notify. If it is notifiable, the PDPC must be told as soon as practicable and within 3 calendar days of that assessment. Staff never make that call themselves.

Not following this policy. A mistake reported promptly is treated as a learning point. Deliberately ignoring the rules, or hiding a mistake, is handled by the HR Manager under the normal disciplinary process.

7. How this policy supports the PDPA programme

PDPA area (B2 gap)	What this policy does	Where the detail is
Accountability (G-01)	A written, owned, approved rule that staff are briefed on	B5 policy, B15 briefing
Purpose limitation (G-03)	Data collected for orders, hiring or service is not reused in AI tools for other purposes	B3 inventory
Protection (G-07)	Bans on high-risk data and personal accounts; tool list kept by IT	B9 vendor checklist
Transfer limitation (G-09)	Personal AI accounts may process data overseas, so personal data stays out of them	B10 transfer checklist
Breach notification (G-10)	Same-day reporting and the B11 assessment and decision steps	B11 breach plan

8. Putting it in place: owners, evidence, next actions

Next action	Owner role	Evidence that it is done	Target
MD approves this policy	Managing Director	Signed v1.0 in the policy folder	13 November 2026

Next action	Owner role	Evidence that it is done	Target
Publish the approved tool list on the intranet	IT Manager	Intranet page and its date	20 November 2026
Block personal AI accounts from opening Quillmarrow SharePoint files where Microsoft 365 allows it	IT Manager, with Fictional Harbour IT	Masked configuration screenshot	15 December 2026
Brief all staff (B15, AI section)	Head of Operations, appointed DPO	Attendance record, about 80 staff	15 December 2026
Ask Fictional Helpdesk and Fictional MailBurst which AI features are on (B9)	IT Manager	Vendor answers filed against B9	15 December 2026
Log AI-related incidents and near-misses separately in the B11 log	Head of Operations, appointed DPO	Incident log category in use	From approval

These actions are tracked in B2 under G-01 (policy and staff communication) and G-07 (protection). The DPO reports progress to the MD in the quarterly update. The policy is reviewed when the AI governance pack is approved, or within six months, whichever is sooner.

This policy draws on the *Model AI Governance Framework, Second Edition* (PDPC and IMDA, January 2020) and the *PDPC Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems* (March 2024). It is practical support, not legal advice; the DPO confirms legal questions with a Singapore-qualified lawyer.

About this sample

Fictional organisation, illustrative only, not a client case study. Quillmarrow Supplies Pte. Ltd., its people, vendors, findings and dates are invented. Nothing in this document reports a client result.

I personally review and sign off every deliverable. You appoint your own DPO. I support them.

This is practical compliance support, not legal advice. For legal advice, use a Singapore-qualified lawyer.

What's not included

- Acting as your DPO. You appoint your own DPO; I prepare the handover and can support them separately.
- Legal advice, legal contract drafting, representation or a guarantee of compliance.
- Forensic investigation, penetration testing, security engineering or implementing changes in live systems.
- A detailed AI governance review or ISO/IEC 42001 readiness check unless separately scoped.
- Ongoing document upkeep after handover, unless agreed through monthly DPO support.
- Healthcare-sector work or on-site delivery.

Questions about this sample: DM @alewyl1 on X, or ask for a free intro call (coffee chat).