PDPA PROGRAMME PACK · B5

Internal data protection 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	B5 · Internal data protection 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. Purpose and scope

This policy sets out what you must do when handling personal data for Quillmarrow Supplies Pte. Ltd. It gives staff practical rules for collecting, using, sharing, protecting and disposing of personal data, and for escalating requests, complaints and incidents.

It applies to all Quillmarrow staff and, where they handle Quillmarrow data, contractors, Fictional Harbour IT and Tanjung Contoh Logistics Sdn. Bhd. Department heads must ensure that the relevant requirements are communicated to people working for them. The IT Manager and the Head of Operations must ensure that service-provider responsibilities are reflected in the relevant instructions and contracts.

This policy applies to information in any form, including information in systems, emails, recordings, photographs, CCTV footage, paper files and conversations. It covers work at the head office, showroom and warehouse, as well as remote work and work carried out by service providers.

The Head of Operations is Quillmarrow's appointed Data Protection Officer (DPO). Contact the DPO at **dpo@quillmarrow.example** if you are unsure how to apply this policy. The DPO will coordinate any legal questions with a Singapore-qualified lawyer.

This policy is presented for Managing Director approval. Controls described as requirements must be implemented and checked; their inclusion here does not mean they are already operating. Open work is tracked in B2.

2. Key terms

- **Personal data:** Data about an individual who can be identified from that data, or from that data together with other information to which Quillmarrow has or is likely to have access. Examples include a customer's name and home delivery address, an applicant's CV and identifiable CCTV footage.
- **Business contact information:** Contact details used to contact a person in their business or official capacity. Such information is treated differently under the PDPA. Do not assume every detail held about a business contact falls into that category; ask the DPO to confirm questions with a Singapore-qualified lawyer.
- **Data intermediary:** An organisation that processes personal data on Quillmarrow's behalf. DV-01, Tanjung Contoh Logistics Sdn. Bhd., and DV-02, Fictional ShopCloud, are identified as data intermediaries in the inventory. The role of another provider depends on its actual activities.
- **Consent:** An individual's agreement to the collection, use or disclosure of their personal data for an identified purpose. A notice and a consent choice are not the same thing.
- **Deemed consent:** A situation in which the law may treat an individual as having consented in particular circumstances. Do not assume it applies merely because information is available or because someone has not objected. Refer questions to the DPO for legal review.

- **Data breach:** An incident involving unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data, or loss of a storage medium or device containing personal data.
- **Notifiable data breach:** A breach that meets the notification criteria in section 7. The DPO and MD assess and record the decision; staff must not make that decision for themselves.

These explanations are for day-to-day use, not legal advice. The DPO should seek confirmation from a Singapore-qualified lawyer when a definition or its application matters to a decision.

3. Roles and responsibilities

Role	Responsibilities
Managing Director (MD)	Approves this policy, the B11 breach management plan and the final pack. With the DPO, records the notification decision described in B11. Ensures management decisions and resources are considered.
Chief Operating Officer (COO)	Sponsors the programme, supports cross-department action and receives progress and escalations.
DPO — Head of Operations, appointed by Quillmarrow	Owns the programme day to day; maintains this policy and the action tracker; coordinates requests, complaints, breach assessment and advice; and reviews the inventory with owners.
Department heads	Apply the policy in their areas, identify data and purposes, maintain appropriate access, support requests and incidents, and complete assigned actions.
IT Manager	Coordinates Fictional Harbour IT, system security, access reviews, configuration evidence and technical support for containment and requests.
All staff	Follow this policy, use approved processes, complete training, protect data and report concerns immediately.
Data intermediaries and other relevant service providers	Handle Quillmarrow data only under agreed instructions and contractual arrangements; protect it, support requests and report suspected incidents through the agreed route.

Appointing a DPO does not remove Quillmarrow's obligations. The organisation remains responsible for its decisions and for ensuring that assigned controls are put into practice.

4. The obligations in practice

4.1 Consent

- Collect, use or share personal data only for an identified purpose and through an approved process. If you are unsure what permits the activity, ask the DPO before proceeding.
- Use a separate, optional and unticked choice for marketing where the approved process requires consent. Do not treat an order or service request as agreement to unrelated marketing.
- Record the choice, the purpose, the collection point and the date in the approved system. Do not create a consent record for a past choice if no evidence exists.
- Pass a withdrawal to the Head of Marketing promptly and update the relevant list and suppression records. Ask the DPO about effects on other uses.

Linked documents: B3 inventory, B4 notices and B6 consent materials. G-02 includes the pre-ticked B2B marketing box and missing showroom consent records; follow the B2 action plan.

4.2 Purpose limitation

- Before collecting information, identify the business purpose and collect only what is needed for it.
- Use the information for the stated purpose and any other use approved through the DPO's review. Do not invent a new purpose because the data is convenient to access.
- Ask the DPO before reusing data for a materially different purpose. The DPO will arrange legal review where needed and update notices or processes as appropriate.
- Do not use showroom CCTV for staff timekeeping or another purpose outside its stated purpose without an approved review. The previous timekeeping use is recorded under G-03.

Linked documents: B3 inventory and B4 notices. Department heads should tell the DPO when a purpose changes.

4.3 Notification

- Give people the relevant approved privacy notice at the point where their information is collected, before they submit it.
- Use the checkout notice for web-shop customers and the application notice for applicants once approved and published. Do not copy one notice to a different collection point without review.
- Tell the DPO if a notice, link or contact detail is missing, inaccurate or difficult to find. Do not promise a practice that Quillmarrow has not confirmed.
- Ask the DPO to review notices when data, purposes, recipients or collection methods change. Keep evidence of the version and where it was displayed.

Linked documents: B4 notices and B3 inventory. The job-application, showroom sign-up and CCTV notice gaps are tracked under G-04 in B2.

4.4 Access and correction

- Send any request to see or correct personal data to the DPO and Head of Customer Service promptly, including a request received verbally or through a vendor.
- Record the request in the B7 log. The proposed service targets are to acknowledge within three working days and respond within 30 days; these are Quillmarrow's targets, not permission to delay a response that can be made sooner.
- Verify the requester's identity using the approved process and locate relevant records without collecting more information than necessary. Do not disclose another person's information simply because it appears in the same record.
- If more time is needed, tell the person in writing within 30 days when a response will be given. The DPO should confirm the applicable approach with a Singapore-qualified lawyer.
- Record the decision, response and any correction. Escalate requests involving third-party CCTV footage, such as AR-04, and requests received by DV-01, such as AR-06.

Linked documents: B7 request log and process, and B3 inventory. G-05 records that requests have been handled ad hoc and one took 41 days.

4.5 Accuracy

- Take reasonable steps to check information when accuracy matters to the intended use, especially before using it to make a decision or disclose it.
- Follow the B2B onboarding verification and annual Sales check for account details. Record the check and update the relevant system when a correction is confirmed.
- Tell the DPO if you find conflicting or unreliable information that could affect an individual. Do not silently overwrite a disputed record where the history needs to be preserved.
- Correct information through the approved process and consider whether recipients need to receive the correction. Ask the DPO if the next step is unclear.

Linked documents: B3 inventory and B7 request records. G-06 records the reported B2B checks; owners should retain evidence that they continue.

4.6 Protection

- Access personal data only when you need it for your work. Do not browse customer, employee or applicant records out of curiosity.
- Use approved accounts, storage and sharing settings. Check the recipient and content before sending a message, file or link.
- Protect accounts with MFA where available and required. Do not share passwords or approve an unexpected sign-in request.
- The IT Manager must arrange access reviews, including administrator access held by DV-03, Fictional Harbour IT. Remove or adjust access through the approved process when a role changes.
- Report a wrong recipient, exposed link, lost device or unusual access immediately under section 7. Do not wait for proof that someone misused the data.

Linked documents: B3 inventory, B9 vendor questionnaire and B10 security materials. G-07 tracks the sharing near-miss, missing ShopCloud admin MFA and unreviewed MSP access.

4.7 Retention limitation

- Keep records only in approved locations and follow the retention decision for the relevant record type in B8 once Quillmarrow has confirmed it.
- Do not assume a proposed period in B8 has already been approved. If there is no decision, tell the record owner and DPO; do not invent one.
- Review records due for disposal and follow the approved deletion or secure-disposal process. Record the action and any exception.
- Pause routine disposal where the DPO or relevant owner has identified a complaint, investigation, dispute or other hold. Record the reason and review date.
- Ask the Finance Director to confirm accounting and tax retention requirements with the accountant or lawyer. Do not treat a generic schedule as proof of a statutory period.

Linked documents: B8 retention schedule and B3 inventory. G-08 records the absence of an approved schedule. The reported CCTV overwrite setting must be checked.

4.8 Transfer limitation

- Tell the DPO before arranging a new overseas transfer or changing a provider, hosting location or support arrangement that may involve overseas access.
- Record the data, destination, recipient, purpose and proposed safeguards in the B3 inventory and B9 vendor records.
- For Malaysia deliveries, use only the approved information and route for DV-01. Do not assume that the existing confidentiality clause resolves all transfer questions.
- Ask the IT Manager to confirm DV-02's hosting region and any relevant support locations. Do not describe ShopCloud as hosted in a particular region until evidence is available.
- The DPO should assess safeguards and seek advice from a Singapore-qualified lawyer. The ASEAN Model Contractual Clauses are one option for consideration, not a substitute for reviewing the actual arrangement.

Linked documents: B3 inventory and B9 vendor questionnaire. G-09 and the relevant actions remain open in B2.

4.9 Data breach notification

- Report a suspected or confirmed breach immediately as set out in section 7. Your first task is to raise the alarm, not to determine whether notification is required.
- Help the DPO establish the facts, affected data, scale and possible harm. Preserve relevant records and do not alter or delete evidence unless directed as part of containment.
- Follow B11 for containment, assessment, the separate notification decision, communications and lessons.
- Refer external enquiries to the DPO or the person authorised under B11. Do not promise that an incident is harmless or that no notification will be made.

Linked document: B11 breach management plan. G-10 records that the existing near-miss was handled by email and that a plan, assessment form and decision log were missing.

4.10 Accountability

- Know who owns the records and processes you use. Tell your department head and the DPO when a new system, vendor, collection point or purpose is proposed.
- Keep evidence of decisions and completed controls, such as notice versions, access reviews, training and approved retention actions.
- Complete assigned B2 actions by their agreed target dates, or tell the DPO promptly if a date or dependency is at risk.
- Cooperate with reviews and correct gaps. Do not mark an action complete solely because a document has been drafted.

Linked documents: B2 action tracker, B3 inventory, B9 vendor records and this policy. G-01 includes publication of the DPO contact and staff communication.

5. Do Not Call

Do not conduct telemarketing to Singapore numbers without following the **B12 process**. Before any campaign, the Head of Marketing must confirm the audience, proposed message, sender details, suppression process and the DNC register-check or other applicable basis with the DPO.

Where a register check is required, use it **within the validity period set by the PDPC (confirm the current period)**. Keep the relevant check and campaign records under RS-08 once the retention decision is confirmed. Do not rely on a prospect list merely because it was supplied by a third party or contains business contacts.

The planned campaign and missing register-check process are tracked under G-11. The DPO should refer legal questions, including whether an exception applies, to a Singapore-qualified lawyer before the campaign proceeds. Refer to the PDPC Advisory Guidelines on the Do Not Call Provisions.

6. Everyday security rules

- **SharePoint links:** “Anyone with the link” sharing must be off by default. Use named-person or other approved restricted access. The IT Manager must confirm and evidence the setting; do not assume it is already configured.
- **MFA:** Use MFA on work accounts where required. The IT Manager must address the reported absence of MFA on Fictional ShopCloud administrator accounts and record the outcome under G-07.
- **Clean desk:** Put paper records and removable media away securely when not in use. Use approved secure disposal for material no longer needed.
- **Lock screens:** Lock your screen when leaving your device. Do not leave personal data visible to visitors or unauthorised colleagues.
- **Approved tools only:** Use systems and storage approved for the work. Do not create an unreviewed account or upload records to an unapproved service.
- **No personal email:** Do not send work data to a personal email account or use one to carry out Quillmarrow business.
- **AI tools:** Follow B14 before using ChatGPT, Copilot or another AI tool with work information. Do not enter personal data into a tool unless the use has been specifically reviewed and approved through Quillmarrow’s process.
- **Physical handling:** Check labels and recipients before dispatching documents or parcels. Report a misplaced record or delivery immediately.

The IT Manager should provide practical instructions for these rules and retain configuration and review evidence. The DPO should track implementation through B2.

7. Reporting incidents

Report a suspected or confirmed personal data breach **immediately** to the DPO at **dpo@quillmarrow.example** and alert your department head. If the DPO is unavailable, alert the MD and IT Manager promptly so that containment can begin. Provide what you know: what happened, when you noticed it, the systems or records involved, who may have received access and any immediate action taken.

Do not wait to collect every detail. Do not conceal a mistake, contact affected individuals on your own initiative or delete evidence. Follow instructions to contain the incident safely. Staff do not decide whether a breach is notifiable; the DPO and MD follow B11 and record the assessment and decision separately.

The breach rule is:

- A data breach is notifiable if it results in, or is likely to result in, significant harm to affected individuals, or is of a significant scale (affects 500 or more individuals).
- The organisation must assess whether a breach is notifiable in a reasonable and expeditious manner; PDPC guidance expects the assessment within 30 calendar days of credible grounds to believe a breach occurred.
- If notifiable, notify the PDPC as soon as practicable and no later than 3 calendar days after assessing that the breach is notifiable.
- Where significant harm is likely, notify affected individuals as soon as practicable, on or after notifying the PDPC, subject to the exceptions in the Act.
- A data intermediary processing on Quillmarrow's behalf must notify Quillmarrow without undue delay after it has credible grounds to believe a breach occurred.
- Keep the assessment (facts, scale, harm) separate from the decision to notify (who decides, when, reasons).

- Public explanation: https://alexlew.live/faq.html#faq-breach-deadlines

The DPO should use B11 and seek advice from a Singapore-qualified lawyer where the rule or its application is uncertain. The **PDPC Guide on Managing and Notifying Data Breaches under the PDPA** provides the C.A.R.E. approach: Contain, Assess, Report and Evaluate.

8. Complaints

Send a privacy complaint to the DPO promptly, whether it arrives through a form, email, telephone call, in person or through a provider. Record the date, contact details, issue, responsible owner, actions and response in the approved record for PD-25. Do not record unnecessary sensitive detail.

Acknowledge the complaint, investigate with the relevant department and keep the person informed where appropriate. Escalate a suspected breach under section 7 as well; logging a complaint is not a substitute for immediate incident reporting. The DPO coordinates the response and seeks legal advice where needed.

9. Training and acknowledgement

Department heads must ensure that staff receive this policy and understand the rules relevant to their work. The DPO coordinates induction and refresher training, with additional guidance for people handling recruitment, marketing, customer requests, administration or incidents.

You must complete assigned training, ask when a process is unclear and acknowledge that you have received and understood the policy. The DPO should retain training and acknowledgement records and follow up gaps. Contractors and service providers should receive relevant instructions through their owners and contractual arrangements.

10. Breaches of this policy

Report a suspected breach of this policy to your department head or the DPO. Prompt reporting helps Quillmarrow contain a problem and understand what happened. Do not discourage someone from raising a concern.

The relevant manager and DPO will review the facts, preserve appropriate records and decide the next steps. Depending on the circumstances, these may include further training, changes to access or processes, or action under Quillmarrow's applicable employment or contractual procedures. A policy breach may also require the incident process in B11.

11. Document control

The **DPO, Head of Operations**, owns this policy. The **MD** is the approver. The DPO will review it at least annually and when there is a material change to Quillmarrow's data use, systems, suppliers, legal guidance or an incident lesson. Department heads must help check that the policy remains practical and reflects actual processes.

Version	Date	Description	Owner	Approval status
1.0	30 October 2026	Policy prepared for management review and approval	DPO, Head of Operations	Pending MD approval

Approved by: Managing Director (role) - date to be entered on approval.

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).