PDPA PROGRAMME PACK · B15

# Remote staff briefing: outline and speaker notes

**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** | B15 · Remote staff briefing: outline and speaker notes |
| **Version** | 1.0 |
| **Date** | 30 October 2026 (illustrative) |
| **Prepared by** | Alex Lew, reviewer and sign-off |
| **Client approver (role)** | Head of Operations (DPO) |
| **Label** | Fictional organisation, illustrative only, not a client case study |

## Session plan

**Audience:** All staff, including staff who handle customer, applicant, employee, supplier and visitor information.

**Length:** 45 minutes by video call. Allow approximately 35 minutes for the slides and discussion, and 10 minutes for the knowledge check and questions.

**Presenter:** The Head of Operations, Quillmarrow's appointed Data Protection Officer (DPO), with the reviewer supporting.

**Materials:** This slide outline, the relevant pack documents and the knowledge check below. Use invented or masked examples; do not display customer databases or unmasked personal data during the call.

**Attendance:** HR keeps the attendance record, including the session date, attendees and any follow-up needed for staff who could not attend. The HR Manager and DPO should agree where the record is kept and how long it is needed, in line with B8.

This is an illustrative briefing outline. Proposed notices, procedures and controls should be confirmed and made available before staff are told that they are in operation. Where a legal question arises, the DPO should seek advice from a Singapore-qualified lawyer.

## Slide 1: Why this matters to us

**On the slide:**

- Personal data is part of everyday work.
- People trust us with their information.
- Small mistakes can affect customers and colleagues.
- Ask when you are unsure.

**Speaker notes:**

Quillmarrow handles information when taking orders, helping customers, recruiting staff and receiving visitors. A delivery address or a customer conversation may seem routine, but the person concerned may be affected if it is lost or shared inappropriately. This briefing explains what staff should do and who can help. It is about practical habits, not blaming people for raising a concern.

## Slide 2: What counts as personal data here

**On the slide:**

- Customer names, addresses and mobile numbers.

- Order details and helpdesk conversations.
- Staff records and job applications.
- CCTV footage and visitor logs.

**Speaker notes:**

Personal data can identify someone on its own or when combined with other information. Quillmarrow examples include web-shop orders and delivery details in **PD-02**, helpdesk tickets in **PD-06**, job applications in **PD-15** and showroom CCTV footage in **PD-13**. A spreadsheet without names may still identify people through a combination of details, so ask the DPO before assuming it is anonymous. The B3 inventory describes where information is used and who is responsible for it.

## Slide 3: Our DPO and how to reach them

**On the slide:**

- The Head of Operations is our DPO.
- Raise questions, requests and concerns promptly.
- Contact: dpo@quillmarrow.example.
- The DPO contact is to be published on the website.

**Speaker notes:**

The DPO coordinates Quillmarrow's data protection programme and helps staff handle questions and incidents. Contact the DPO if you receive a request for information, are unsure about a new use of data or suspect a mistake. The business contact is **dpo@quillmarrow.example**; its website publication is an outstanding action under **G-01**, not something staff should assume has happened. The reviewer supports the programme, but is not Quillmarrow's DPO.

## Slide 4: Collecting data: notices and consent

**On the slide:**

- Explain why information is collected.
- Collect only what is needed.
- Do not pre-tick a marketing consent box.
- Record and respect consent choices.

**Speaker notes:**

Use the relevant approved notice when asking for information, and make sure it describes the purpose in plain language. The review found a pre-ticked marketing box on the B2B account form and no consent records for showroom sign-ups; these are gaps to address under **G-02** and **G-04**. Do not assume that a person who gives details for an order has also agreed to marketing. Follow B4 for notices and B6 for consent and withdrawal once those procedures are approved and put into use.

## Slide 5: Marketing and DNC

**On the slide:**

- Check the purpose, list and channel.
- Follow the DNC process before a campaign.
- Include the required sender details.
- Record and act on opt-outs.

**Speaker notes:**

The planned campaign to SME owners uses the prospect list in **PD-10** and needs a documented review before messages or calls are released. Do not assume that a mobile number can be used for marketing because it was found online or belongs to a business contact. Follow B12 for list sources, consent evidence, sender details and the relevant register check **within the validity period set by the PDPC (confirm the current period)**. Refer uncertain cases to the DPO, who should confirm legal questions with a Singapore-qualified lawyer.

## Slide 6: When someone asks for their data

**On the slide:**

- Recognise and forward the request.
- A person need not use a special form.
- Do not send records without checks.
- Follow B7 and record the request.

**Speaker notes:**

A request may arrive by email, telephone, in person or through the Malaysia partner, as illustrated by **AR-06**. Forward it promptly to the DPO and the appropriate intake team; Customer Service handles customer and general intake, while HR handles staff and applicant intake. Verify identity and consult the DPO before disclosing records, especially where information about other people may be visible. B7 sets an internal acknowledgement target of three working days and a response target of 30 days; the DPO should confirm the legal requirements and any extension wording with a lawyer.

## Slide 7: Keeping data safe day to day

**On the slide:**

- Check the recipient before sharing.
- Use the narrowest appropriate access.
- Avoid open links for customer records.
- Report a mistake without delay.

**Speaker notes:**

In the illustrative SharePoint near-miss, a folder containing customer and business contact records was shared through an “anyone with the link” setting and the link was sent to an external courier contact by mistake. The link was removed, and the incident was assessed; the purpose of discussing it is to learn, not assign blame. Before sharing, check the folder contents, recipient and permissions, and use only the access needed for the task. The IT Manager should confirm the actual sharing settings and proposed fixes under **G-07**.

## Slide 8: Vendors and Malaysia

**On the slide:**

- Use vendors only for an agreed purpose.
- Share only the information needed.
- Malaysia delivery records go to DV-01.
- Ask before a new transfer or vendor use.

**Speaker notes:**

Tanjung Contoh Logistics, **DV-01**, receives Malaysia order and delivery information for fulfilment, including **PD-11**. Its contract has a confidentiality clause but no data protection clauses; the proposed safeguards and contract work remain open under **G-09**. Do not assume that every file or field can be sent simply because a vendor is already engaged. Refer a proposed change to the DPO and use B9 and B10 to record the vendor review and transfer questions.

## Slide 9: Keeping and deleting

**On the slide:**

- Do not keep everything indefinitely.
- Follow an approved retention decision.
- Check for a hold before deletion.
- Include vendor-held copies.

**Speaker notes:**

The review found no retention schedule in operation, with records generally kept indefinitely; the reported CCTV overwrite setting is about 30 days but needs verification. B8 sets out proposed decisions for the organisation to confirm, not universal periods that staff should apply automatically. Before deleting, check the record type, approved trigger and any instruction to preserve information for a dispute or investigation. Ask the DPO about copies held by providers, including Malaysia delivery records under **RS-20**.

## Slide 10: Spotting and reporting a breach

**On the slide:**

- Report a suspected breach immediately.
- Tell the DPO and IT Manager what happened.
- Preserve relevant information; do not hide it.
- The DPO coordinates assessment under B11.

**Speaker notes:**

A breach may involve information being sent to the wrong person, exposed through a link, lost or accessed without permission. Staff should report immediately and give the DPO and IT Manager the known facts, without waiting to establish every detail.

Walk through INC-2026-07 as the example. The folder was found open at 10:20 on Monday 14 September and the link was removed at 10:45. The DPO assessed the facts from 14 to 16 September: 140 customers' home addresses and mobile numbers were exposed, plus business contact information, and the link was opened twice by one courier who later confirmed deletion. That is below 500 people, and no data of the kinds prescribed as likely to cause significant harm was involved. Then, as a separate recorded step, the MD and DPO decided on 16 September that it was not notifiable.

**The rule staff should remember:** a breach is notifiable if it is likely to cause significant harm, or affects 500 or more people. If it is notifiable, the PDPC must be told as soon as practicable and within 3 calendar days of assessing it as notifiable. Had INC-2026-07 been notifiable, that deadline would have been 19 September. Staff do not make the assessment or the decision; their job is to report fast so the clock is not wasted.

## Slide 11: AI tools

**On the slide:**

- Use tools only for approved purposes.
- Do not enter prohibited information.
- Check every output before use.
- Report mistakes to the DPO and IT Manager.

**Speaker notes:**

B14 sets the basic rules. Microsoft 365 Copilot on the company licence is allowed for internal drafting and summaries that staff then check. Vendor AI features are used only when the IT Manager has listed them. Personal ChatGPT accounts are for general questions only, with no Quillmarrow information at all. Never put NRIC or FIN numbers, payment details, CVs, medical records, whole customer or prospect exports, or confidential contract terms into any AI tool. Check every output for facts, prices, personal data and promises, and never let AI decide anything about a person. If something goes wrong, tell the DPO and IT Manager the same day.

## Slide 12: Recap and where to find things

**On the slide:**

- Collect and share only what is needed.
- Recognise requests and report concerns.
- Use the approved pack documents.
- Ask the DPO when unsure.

**Speaker notes:**

The main habits are to understand the purpose, check access, respect choices and escalate promptly. B4 covers notices, B6 consent, B7 requests, B8 retention, B11 incidents, B12 DNC and B14 basic AI use. The DPO should tell staff where the approved versions are kept and identify any documents still awaiting approval or implementation. Use the questions below to check understanding and note any topics that need follow-up.

## Knowledge check

**1. A colleague asks for a customer spreadsheet to help with a delivery. What should you do first?**

A. Send an open link because the request is work-related.
B. Check what information and access the colleague needs, then use an appropriate sharing method.
C. Send the whole customer database to save time.

**Correct answer: B.** Check the purpose, recipient and permissions, and share only what is needed.

**2. A customer asks by telephone for a copy of their order information. What should you do?**

A. Ignore the request because it was not made on a form.
B. Read out all available details immediately.
C. Forward and record the request under B7, with identity checks before disclosure.

**Correct answer: C.** A special form is not required, and identity and disclosure checks are needed.

**3. A marketing colleague has an old list of SME owners' mobile numbers. Can they start calling immediately?**

A. Yes, because the numbers relate to businesses.
B. No; the list, evidence, channel and relevant DNC checks need review under B12.
C. Yes, if the message includes a product offer.

**Correct answer: B.** A business context or an old list does not by itself establish that the campaign can proceed.

**4. You discover that you sent a customer file to the wrong recipient. What should you do?**

A. Report it immediately to the DPO and IT Manager and preserve the relevant facts.
B. Wait until you know for certain that the recipient opened it.
C. Delete your sent message and say nothing.

**Correct answer: A.** Prompt reporting allows the organisation to contain and assess the incident under B11.

**5. An AI tool drafts a product description for you. What should you do before using it?**

A. Publish it because the tool produced it.
B. Check its accuracy, personal data, product claims and prices against approved information.
C. Ask the tool whether it is correct and rely on its answer.

**Correct answer: B.** Staff remain responsible for checking an output before sharing or acting on it.

## After the session: owners, evidence and next actions

| Action | Owner role | Evidence | Target |
|---|---|---|---|
| Run the session for all staff (two slots to cover shifts at the showroom and warehouse) | Head of Operations, appointed DPO | Session dates and slides version | 15 December 2026 |
| Record attendance and chase anyone who missed it | HR Manager | Attendance record, about 80 staff | 22 December 2026 |
| Score the knowledge check; repeat the topic for any question most people got wrong | Head of Operations, appointed DPO | Scores summary in B2 under G-01 | 22 December 2026 |
| Add the briefing to onboarding for new joiners | HR Manager | Onboarding checklist updated | 31 January 2027 |
| Repeat yearly, and after any notifiable breach or major process change | Head of Operations, appointed DPO | Next session date in the B16 calendar | Annually |

Closing G-01's staff-communication item in B2 needs the attendance record and the scores summary, not just the slides.

## 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).