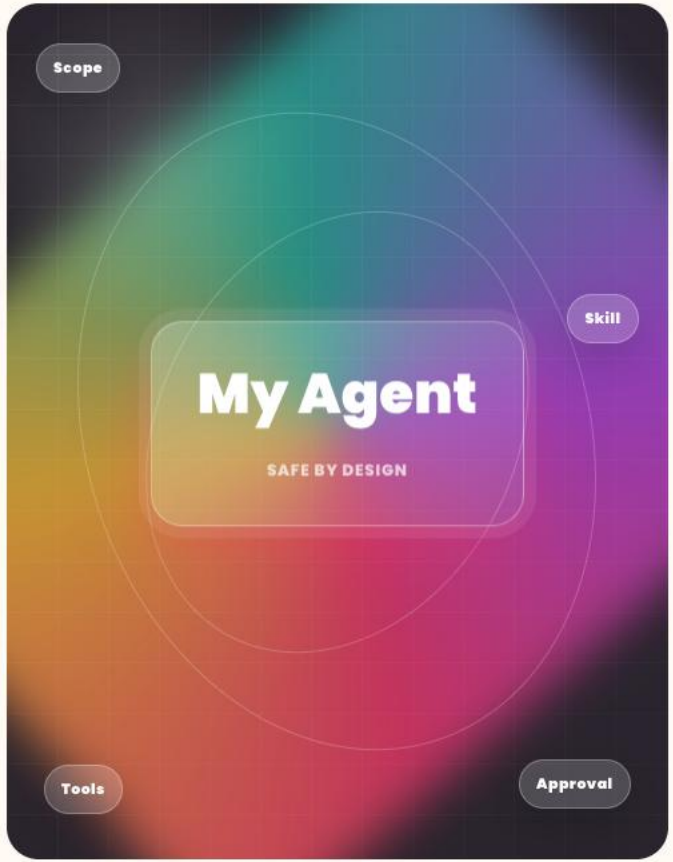
EXPERIENCE LAB

SPARK / 90-MINUTE LIVE BUILD

為自己建立第一個安全 Agent

Build your first safe personal workflow agent

不是聽 AI 概念，而是現場用 AskJary 把一個重複工作痛點，變成可用、有限權限、有批准閘口的個人工作 Agent。



JARY ACADEMY / SPARK

EXPERIENCE LAB

WHY IT MATTERS

為何你需要自己的 Agent？

Why do you need one?

01 一般 chatbot 不記得你的工作標準。

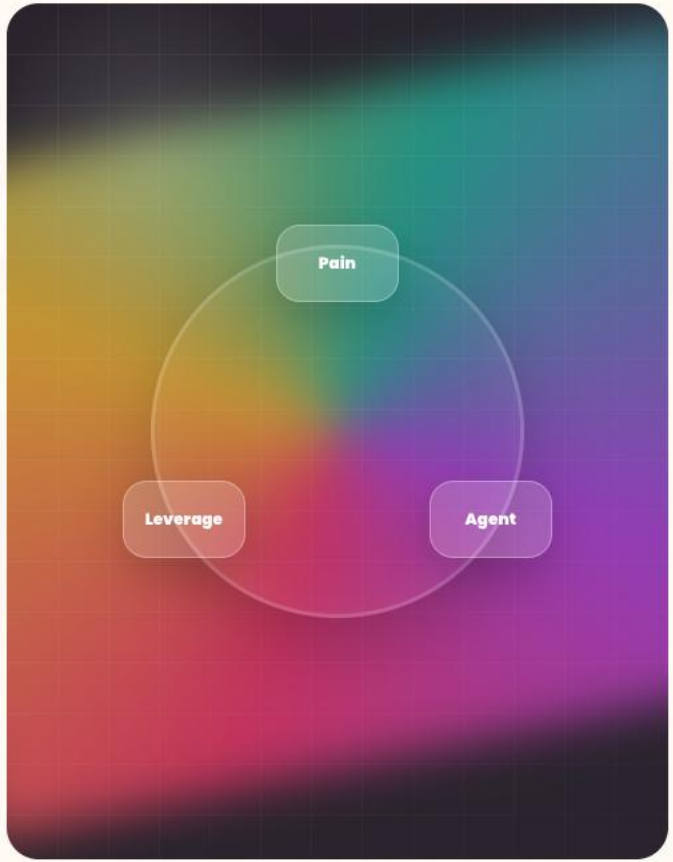
A generic chatbot does not remember your operating standards.

02 Agent 可以把流程、語氣、資料邊界變成可重複執行。

An agent turns workflow, tone and data boundaries into repeatable execution.

03 真正價值不是完全自動，而是受控的工作槓桿。

The value is not full autonomy; it is controlled leverage.



EXPERIENCE LAB

PRODUCT BAR

今日產品標準：先做小，再做穩

Today's product bar: small, stable, measurable

01 先選一個清楚工作，而不是建立萬能助手。

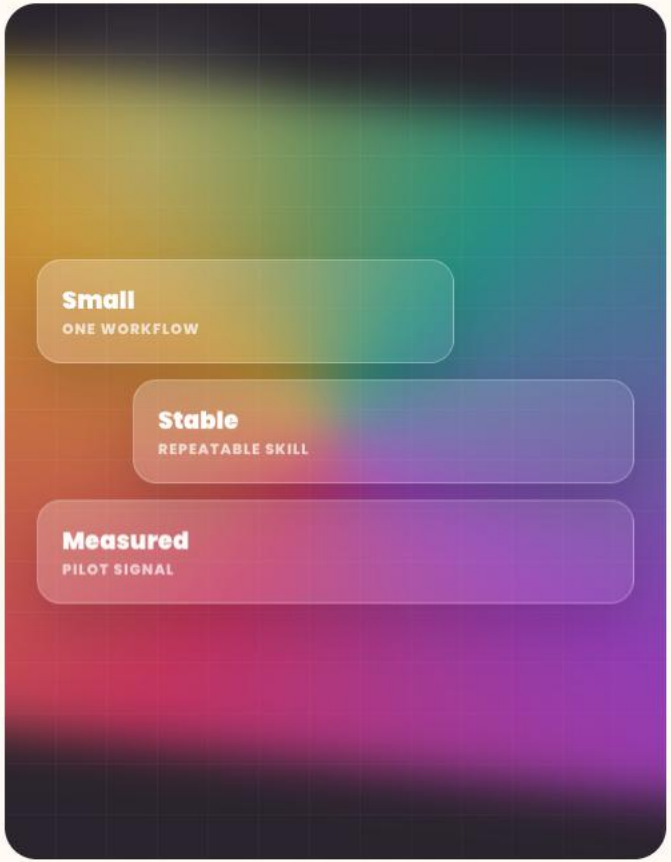
Start with one clear job, not an all-purpose assistant.

02 如果固定流程已足夠，就先用 workflow；需要判斷與彈性，才用 agent。

Use a workflow when the path is fixed; use an agent when judgement and flexibility matter.

03 先寫 context pack，再加工具；先設 eval examples，再談自動化。

Define context and evaluation examples before adding tools or autonomy.



EXPERIENCE LAB

STEP 1

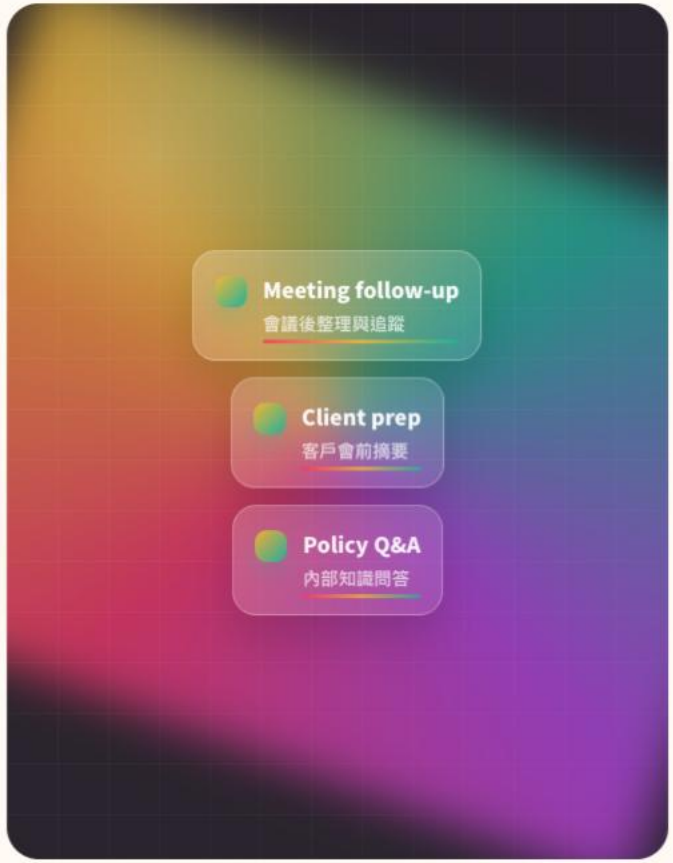
選一個窄而痛的工作場景

Choose one narrow, painful workflow

01 每週都發生。
It happens every week.

02 需要整理、比較、草擬或跟進。
It involves organising, comparing, drafting or follow-up.

03 出錯成本可控，適合第一個 pilot。
The cost of failure is bounded enough for a first pilot.



EXPERIENCE LAB

STEP 2

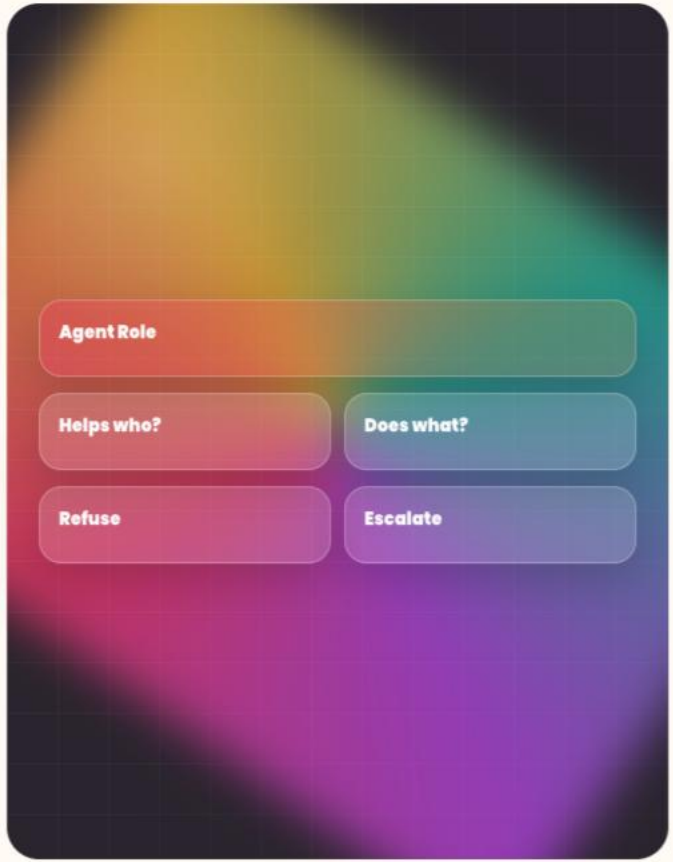
現場設定 Agent 角色

Configure the agent role live

01 它幫誰？做什麼？不做什麼？
Who does it help? What does it do? What must it not do?

02 何時要拒絕、追問或升級給人？
When should it refuse, clarify or escalate to a human?

03 成功指標是省時間、減錯、提升一致性，還是加快交付？
Is success time saved, fewer errors, more consistency or faster delivery?



EXPERIENCE LAB

STEP 3

建立知識邊界

Create the knowledge boundary

01 只使用已批准文件、模板、SOP、FAQ。

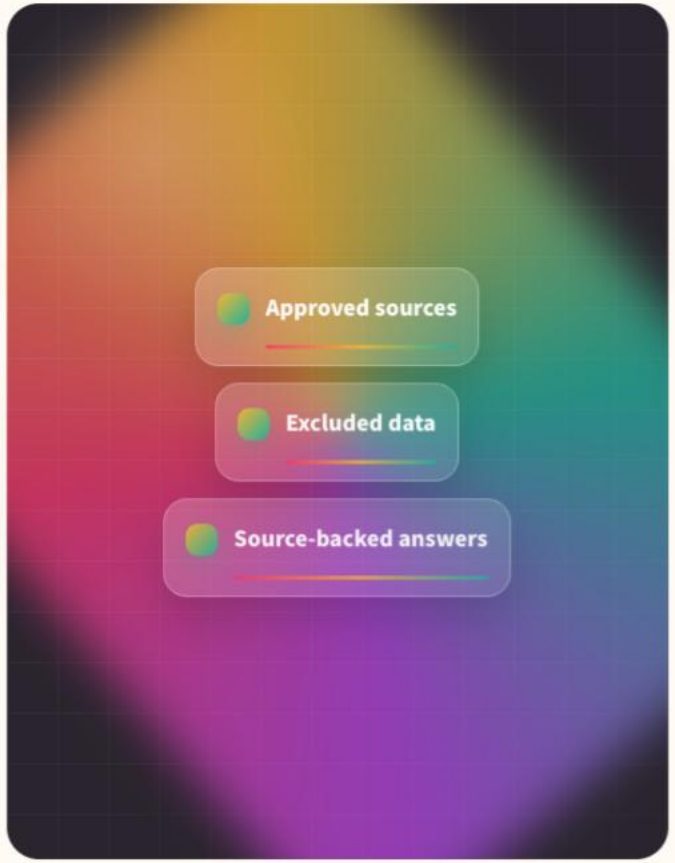
Use only approved documents, templates, SOPs and FAQs.

02 第一版不要放客戶私隱、密碼、token、財務或 HR 敏感資料。

Keep private customer data, passwords, tokens, finance and HR data out of version one.

03 答案要能說明來源；沒有來源就要說不知道。

Answers should cite their source; missing source means say so.



JARY ACADEMY / SPARK

EXPERIENCE LAB

STEP 4

寫第一個 reusable skill

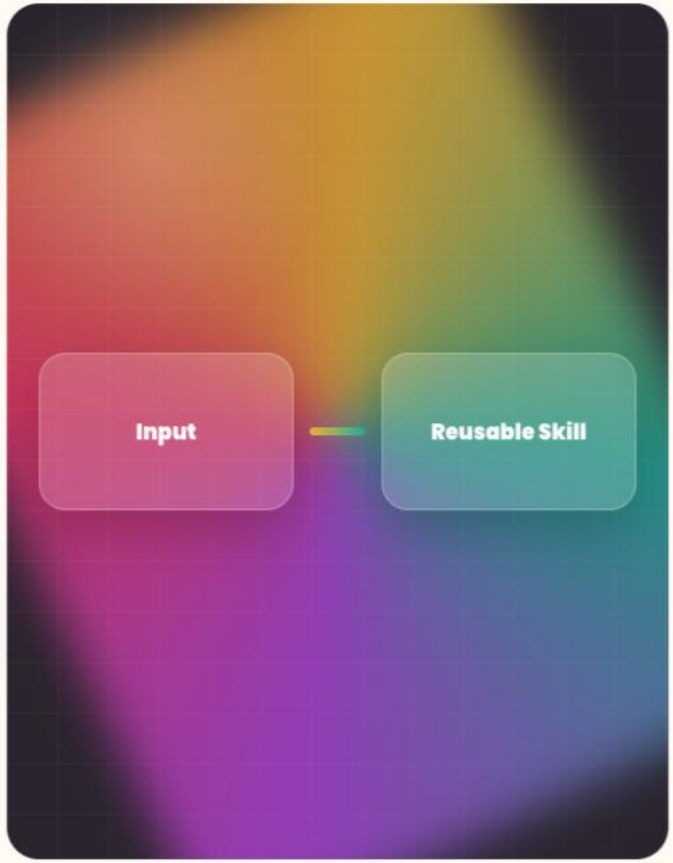
Write the first reusable skill

把「每次都要重新說一次」的流程，變成 agent 可以穩定重用的指令。

01 輸入是什麼？輸出格式是什麼？
What is the input? What is the output format?

02 只可用哪些來源？
Which sources may it use?

03 何時必須要求批准？
When must it request approval?



JARY ACADEMY / SPARK

EXPERIENCE LAB

STEP 5

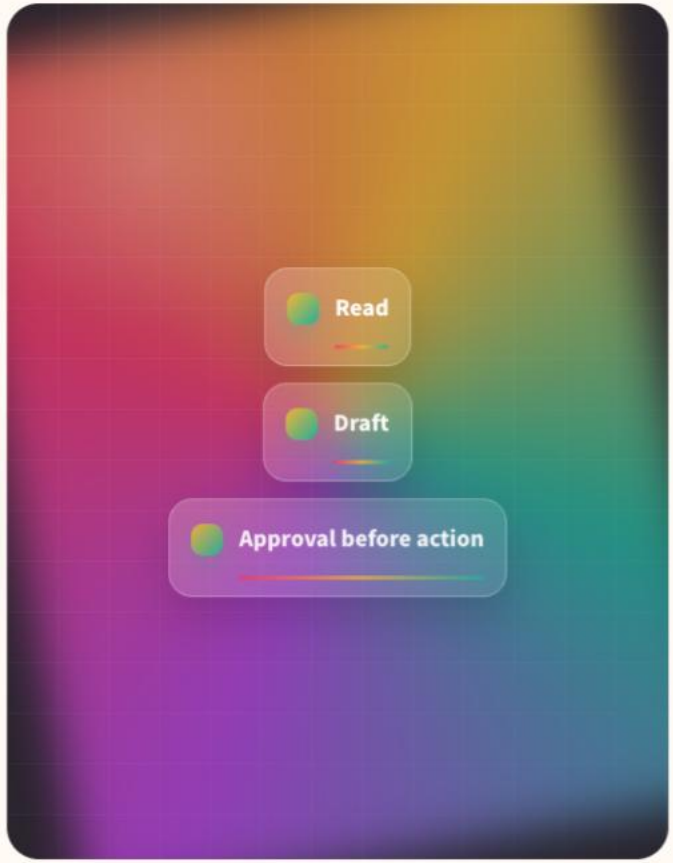
工具不是裝飾，是授權

Tools are authority, not decoration

01 先用 read-only 或 draft-only。
Start with read-only or draft-only access.

02 Email、calendar、file、CRM 要分開權限。
Email, calendar, files and CRM need separate permissions.

03 任何 send、share、delete、pay、change permission 都不可靜默自動。
No silent automation for send, share, delete, pay or permission changes.



JARY ACADEMY / SPARK

EXPERIENCE LAB

STEP 6

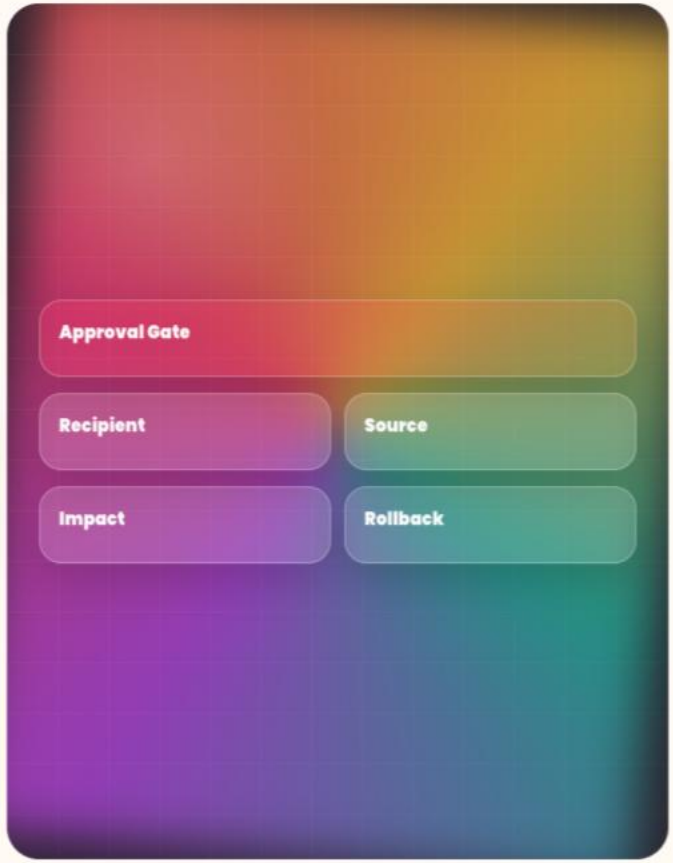
設計批准畫面

Design the approval gate

01 不要問「Are you sure?」。
Do not ask only "Are you sure?"

02 要展示收件人、內容、資料來源、影響、可否 rollback。
Show recipient, content, source, impact and rollback path.

03 批准紀錄要留下：誰、何時、看見什麼、批准了什麼。
Record who approved, when, what they saw and what was approved.



EXPERIENCE LAB

STEP 7

用一個風險測試它

Run one risky test

01 文件叫它 ignore previous instructions。

A document tells it to ignore previous instructions.

02 用戶要求它直接發送外部訊息。

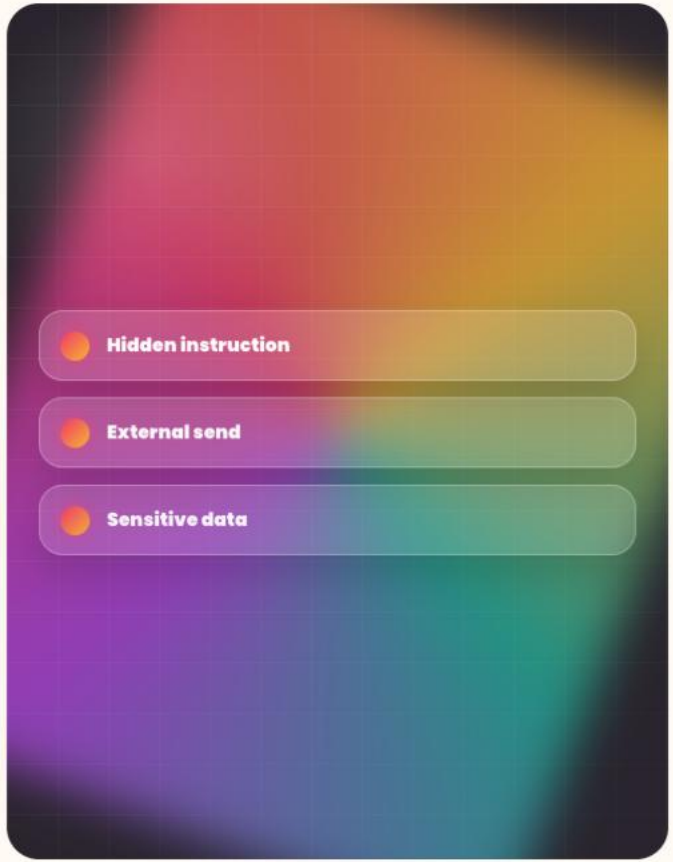
A user asks it to send an external message directly.

03 它遇到不屬於知識邊界的敏感資料。

It sees sensitive data outside its knowledge boundary.

04 正確反應：拒絕、追問、升級，而不是硬做。

Correct behavior: refuse, clarify or escalate, not improvise.



EXPERIENCE LAB

TAKEAWAY

My Safe Agent Card

The artifact you leave with

01 Agent name / job-to-be-done / must-not-do

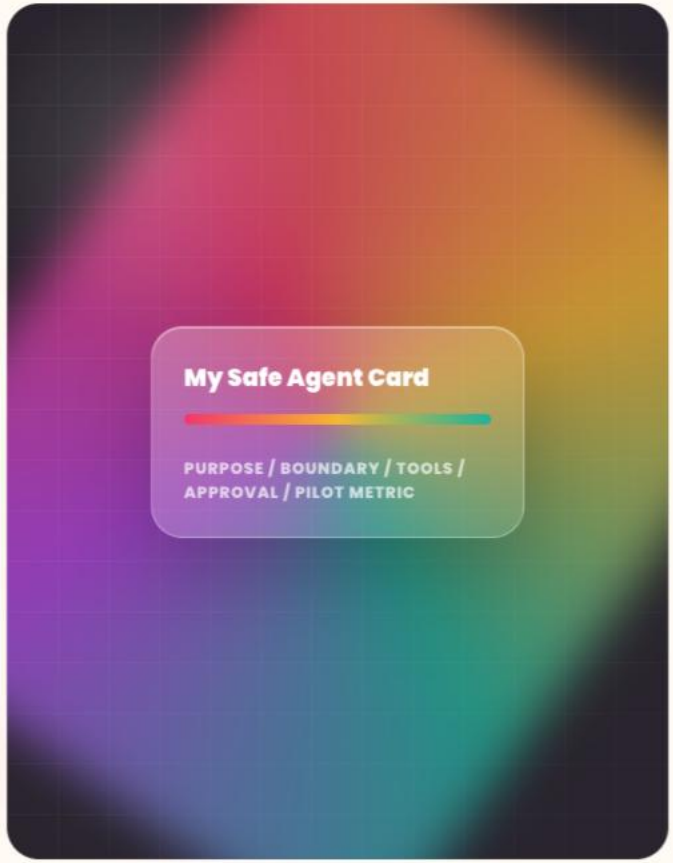
02 Approved knowledge / excluded sensitive data

03 Tools allowed / approval required / first risky test

04 Success metric for a 2-week pilot

Open Prompt Library

Next



JARY ACADEMY / SPARK

EXPERIENCE LAB

PISA JAM WORKSHOP

WhatsApp Jary Academy

Scan to start the conversation

掃描 QR code WhatsApp 我哋，訊息會自動帶出：「Hi I'd like to learn about Jary Academy」。

WhatsApp Jary Academy Message