為什麼台積電(TSMC)不允許員工把工作問題拿去問 LLM？

（也適用於：NVIDIA、Apple、ASML、Google 晶片部門、政府機關、金融業）

編撰：屏東大學 周國華老師 (與 ChatGPT 共筆) 2025/11/26

這是**全球半導體業共同的政策**，原因如下：

❑ 核心原因：保密義務 (NDA) + 商業機密外洩風險

台積電工程師每天接觸的是：

- 製程參數（Process recipes, PDK 資料）
- 光刻條件（EUV/DUV tuning）
- Die layout、IP (Standard cells, SRAM macros)
- 良率數據（Yield）
- 設備參數（ASML、TEL、LAM、AMAT）
- 客戶設計細節（Apple, AMD, NVIDIA）
- 生產排程、產能資訊（非常敏感）
- FAB 事件、WAT data、SPC、瑕疵分析資料

👉 **任何一句話拿去問聊天機器人，都可能被視為機密洩漏。**

例如不要看似無害的問題：

「為什麼我在 N5 製程中，Poly 殘留會造成後段 Cu line collapse？」

這句話就已經洩露：

- 製程節點：N5
- 問題類型：Poly 殘留
- 裝置類型：Cu interconnect
- 可能透露台積最近在解的技術問題

即使沒寫「台積電」三個字，還是具有識別性。

---

❷ 模型供應商可能用這些資料做再訓練（fine-tuning）

雖然像 OpenAI、Anthropic、Google 已經允諾「不使用 API 資料用來訓練模型」，
但：

- **瀏覽器 UI**（chat.openai.com） 未必完全等於 API
- 模型供應商的資料使用條款可能會改
- 公司無法保證資料絕對不會被模型吸收
- 企業需要風險最小化原則（minimum risk）

因此半導體公司採取政策：

只要不能 100% 保證不會進入訓練，就禁止傳。

---

❸ 即使不會被正式訓練，資料仍可能被：

- 儲存在伺服器 log
- QA/Debug 人員直接看到
- 模型公司內部做「安全檢查」
- 第三方承包商接觸到
- 模型回應中「幻覺化」泄漏出去

所有這些情境都可能導致**機密散佈到台積無法控制的環境**。

---

❹ 台積電必須遵守與客戶簽的超高強度保密協議

例如 Apple、NVIDIA、AMD、Qualcomm、MediaTek、Intel…
對台積電的要求都包含：

- 不得將任何客戶資料外傳
- 包含不得輸入第三方 AI 工具
- 包含不得放到雲端合作平台（如 Google Drive）

→ **只要一次違規，TSMC 的商業關係可能出現重大風險**。

5 半導體屬於國家戰略產業（特別是台灣）

輸出製程細節、設備參數、良率資料等，
可能造成：

- 國家安全風險
- 技術外洩（競爭國取得關鍵 know-how）
- 供應鏈被動搖

因此台積電政策極端保守是合理的。

---

6 模型回答可能不準，導致錯誤決策（Quality & Safety Risk）

例如工程師問：

「EUV overlay 失敗，是否與 stage heating 有關？」

模型可能回：

「是的，stage heating 可能造成 overlay error。」

但實際原因可能是：

- Reticle heating
- Dose variation
- Scanner drift
- Pellicle contamination

→ 如果新人信模型的答案去改機台參數，
可能造成：

- 良率暴跌
- 產線事故
- 數千萬美元損失

公司必須避免這種風險。

7️⃣ 模型可能推測出「未公開的商業策略」

例如：

「台積電 2026 年為何要開始 N2 GAA 的 High-NA EUV 設備佈建？」

這類問題可能在無意間揭露：

- 產能佈局
- 技術進程
- 與 ASML 合作內容
- 不對外公開的 roadmap

這也是機密。

8️⃣ 法律與合規（Compliance）要求越來越嚴格

半導體業必須符合：

- 契約 NDA
- IP 受保護資訊（各家 IP vendor）
- 美國出口管制（EAR）
- Cybersecurity 法規
- ISO 27001 資安管理制度

任何資料外傳，都可能違反合規。

✔ 台積電的 AI 使用政策通常會包含：

類型	是否允許	原因
ChatGPT / Gemini / Claude（一般介面）	❌ 禁止	資料會外流至外部雲端
內部部署 LLM（私有雲）	✔ 允許	所有資訊留在台積電封閉網路
API（特殊情況）	⚠️ 需審核	必須確認不會被訓練、不可寫入 log

類型	是否允許	原因
可離線部署的模型（Llama、混合模型）	✔ 可能允許	資料不出廠內

→ 台積電真正想要的是：
完全封閉、不與外界交換資料的 LLM。

🎯 總結

台積電禁止員工把工作問題輸入 LLM，是為了避免商業機密、製程參數、客戶資料外洩，同時遵守 NDA、國家戰略安全、資安法規，以及避免模型給出錯誤建議而造成生產風險。

只有在公司內部部署、完全封閉的 LLM 才可能允許使用。
