
從風險到韌性

學校領導者的網絡安全與人工智能治理

由治理、問責及風險管理出發，避免科技事故演變成學校危機

李安迪校長

危機往往不是突然發生

領導層先問：出事時，我們是否知道怎樣決定？

**如果明天早上8:00，你接到電話：
「學生資料可能已經外洩。」**

第一個電話打給誰？誰有權暫停系統？誰負責通知持份者？

Cybersecurity is not only an IT problem. It is a governance problem.

學校面對「雙重風險」

網絡安全風險

- 帳戶被盜、釣魚及社交工程
- 惡意軟件與勒索攻擊
- 權限設定錯誤及資料外洩
- 第三方供應商及雲端服務風險
- 人為錯誤及欠缺事故匯報

人工智能風險

- 個人資料或機密資料輸入AI
- 幻覺、錯誤資訊及過度依賴
- 偏見、不公平及不可解釋決定
- 版權、知識產權及內容責任
- 供應商、模型及數據管治風險

網絡安全保護系統與資料；AI治理還要保護決策、責任與信任。

由IT管理提升至學校治理

第一層：技術控制

密碼、MFA、備份、權限、防火牆、更新

第二層：管理制度

政策、流程、培訓、供應商管理、事故匯報

第三層：治理與問責

目的、價值、風險承受度、決策權、監督、問責

領導層不需要懂得所有技術，但必須確保每項高風險決定有準則、有負責人、有監察。

領導層先看風險，不要先看技術

Likelihood 可能性

Impact 影響

Control 控制

Owner 負責人

會否發生？

影響學生、教職員、運作及聲譽有多大？

現時如何預防、偵測與應變？

誰擁有決策權及最終責任？

風險優先次序 = 可能性 × 影響 × 現有控制的不足

- 高可能性 × 高影響：優先處理
- 低可能性 × 高影響：建立應變與復原方案
- 高可能性 × 低影響：透過標準程序控制
- 所有重大風險：必須指定Owner及檢視日期

六道治理閘門： 6G School Digital Governance

G1 Purpose

為甚麼要用？

G2 Data

甚麼資料會進入系統？

G3 Risk

最壞情況是甚麼？

G4 Control

如何預防、偵測及應變？

G5 Accountability

誰決定、執行及負責？

G6 Review

如何監察、暫停及改進？

任何一項未能清楚回答，都不應直接進入全面推行。

情境：老師把學生作文上載到免費AI平台

教育目的：希望快速提供個人化回饋

- 工具是否獲學校批准？
- 作文是否包含姓名、班別、學習表現或其他個人資料？
- 平台會否儲存提示及內容，或用作模型訓練？
- AI回饋是否準確、公平及適齡？
- 老師會否核實內容後才交給學生？
- 出現錯誤、偏見或資料外洩時，誰負責匯報及處理？

有Policy，不等於有Governance。治理是把政策變成每天可執行的決定。

風險越高，人為監督越高

低風險

整理公開資料
草擬一般通告
語言潤飾

抽查及監察

中風險

設計教材
分析匿名化學習資料
草擬學生回饋

教師覆核及記錄

高風險

評估學生能力
判斷支援需要
影響升學或重大教育決定

人在環中
人類保留最終決定權

AI可以提出建議，但問責不能外判。

RACI：不要等出事才問「誰負責？」

工作	校長 / 領導層	IT / 技術人員	AI統籌 / 項目負責人	教師 / 使用者	供應商
政策及風險承受度	A	C	R	I	C
風險評估	A	R	R	C	C
培訓及執行	A	C	R	R	I
監察及審核	A	R	R	I	C
事故應變	A	R	R	I	C

A = 最終問責 R = 執行負責 C = 諮詢 I = 知會

2 a.m. test：系統深夜出問題，誰接到第一個電話？

由事故管理走向學校韌性

事故應變 識別 → 遏止 → 匯報 → 調查 → 復原 → 改進

PLAN

識別風險
評估影響
訂定優先次序

IMPLEMENT

政策與控制
培訓與RACI
供應商管理

EVALUATE

監察與審核
事故演練
檢視效能

PROGRESS

修訂政策
改善流程
分享學習

目標不是追求「零風險」，而是建立能預防、承受、應對及復原的學校。

領導者真正要做的三件事

Know the Risk

看見風險

Own the Risk

承擔問責

Manage the Risk

持續管理

**我們不是要停止使用科技，
而是確保科技在清晰目的、適當控制及人類問責下服務教育。**

讓科技服務教育，而不是讓科技風險主導教育。