學校在使用 AI 時的
保障個人資料私隱實務經驗

講者：朱嘉添校長（香港電腦教育學會主席、沙田培英中學校長）

頂層管理導向

制定政策與指引

建立全校 AI 使用規範，涵蓋教學、行政及評估，確保符合《私隱條例》。

數據治理與監督

成立「資訊科技及數字教育委員會」，統籌 AI 發展並定期評估風險。

資源分配

提供安全伺服器或網上平台及數據加密工具。

專業發展

安排 AI 教師工作坊，提升教師的對AI教學及安全意識。

精細化職級存取控管

權限分配原則：按職位敏感度決定 AI 平台上的資料存取權。

一般教師	可獲取通告、時間表、學校中央文件。
科組／部門主管	獲取所屬科組或部門之特定文件。
班主任／專業職級	經審視後獲取學生個人學習歷程、SEN 狀況或健康資料。
管理層（校長／副校長）	有權獲取人事考績、教師意見調查等高度敏感資料。

學生資料分類與使用授權

1

🔴 高敏感資料（極慎重）

特殊教育需要 (SEN)、健康資料。

實務：必須進行加密儲存，並嚴格限制使用場景。

2

🟡 中敏感資料（需授權）

學生課業、作品、活動詳情或成績表現。

實務：必須獲得家長及學生授權方可使用。

3

🟢 低敏感資料

不會辨識學生身份的資料，獲較高自由度使用。

AI 平台選取策略

公開雲端 AI 平台

適用於處理一般不具辨識性的教學資源。

私人雲端／校本 AI 平台

處理學生數據時的首選，以減低私隱外洩風險。

目標：在提升教學效率與降低數據外洩風險之間取得平衡。

AI供應商管理與合約規範

1 釐清責任

與供應商了解數據收集詳情，避免過度收集學生個人資料。

2 合約條文

在合約中明確資料儲存地點及用途，確保不被用於訓練未授權的 AI 模型。

3 持續溝通

要求供應商定期更新安全漏洞並提供合規證明。

家校合作機制

家長參與

制定「家長人工智能教育守則」，增加透明度。

透明化授權

透過通告或家教會平台獲取授權，讓家長清楚了解學校使用 AI 處理學生個人資料的情況。

實務經驗：持續更新與自評

年度更新

AI 使用政策須隨技術發展（如生成式 AI、深偽技術）每年更新。

自評機制

透過校內自評收集前線教師意見，了解實際教學需求與困難。

案例警示

定期分享釣魚電郵或伺服器入侵案例，強化全校警覺性。

應變機制與結語

恆常機制

建立數據外洩處理流程，成立由管理層及IT組組成的緊急應變小組。

應變 SOP

1. 斷開連接
2. 確定範圍
3. 通報 PCPD
4. 通知受影響家長

總結

保護數據不是選擇，而是**各持份者的共同責任**。