



學校數據安全與風險管理

朱嘉添校長，方霆禧副校長



去年157宗資料外泄 涉學校非牟利機構倍增 - 20241023 - 港聞

【明報專訊】私隱專員公署表示，近年涉及學校及非牟利機構的資料外泄事故呈明顯上升趨勢，公署去年接獲157宗資料外泄事故通報，涉及學校及非牟利機構的個案佔61宗，按年升近一倍半；今年首9個月則有51宗來自學校及非牟利機構的通報，佔整體約33%。私...

明報新聞網

資料來源

HTTPS://NEWS.MINGPAO.COM/PNS/%E6%B8%AF%E8%81%9E/ARTICLE/20241023/SO0002/1729620630222/%E5%8E%BB%E5%B9%B4157%E5%AE%97%E8%B3%87%E6%96%99%E5%A4%96%E6%B3%84-%E6%B6%89%E5%AD%B8%E6%A0%A1%E9%9D%9E%E7%89%9F%E5%88%A9%E6%A9%9F%E6%A7%8B%E5%80%8D%E5%A2%9E



港專檔案伺服器被入侵 或部分學校文件或個人資料外洩

香港專業進修學校發言人表示，2月下旬發現遭受高階持續性黑客的勒索軟件攻擊，校方的資訊科技網絡和檔案伺服器被非法入侵，部分文件檔案被盜取及加密，當中或涉及部分學校文件或個人資料外洩。港專發言人說，校方得悉事件後立即採取行動，包括向警方...

Yahoo News

資料來源

HTTPS://HK.NEWS.YAHOO.COM/%E6%B8%AF%E5%B0%88%E6%AA%94%E6%A1%88%E4%BC%BA%E6%9C%8D%E5%99%A8%E8%A2%AB%E5%85%A5%E4%BE%B5-%E6%88%96%E9%83%A8%E5%88%86%E5%AD%B8%E6%A0%A1%E6%96%87%E4%BB%B6%E6%88%96%E5%80%8B%E4%BA%BA%E8%B3%87%E6%96%99%E5%A4%96%E6%B4%A9-130608778.HTML?GUCCOUNTER=1&GUCE_REFERRER=AHROCHM6LY93D3CUZ29VZ2XLLMNVBS8&GUCE_REFERRER_SI

小測試

定期在搜尋器輸入學校的名稱以及自己的名字, 會找到哪些資料?

您有沒有見過學生成就或升學記錄被公開分享
這些資料被洩露會否導致身份盜用或騷擾?
學生的健康資料或特殊教育需要是否可能從第三方平台洩露?



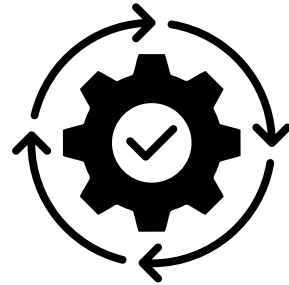
定期使用搜尋引擎檢查個人與學校資料暴露：您可能發現哪些敏感資訊？如何評估其風險並採取防護措施？



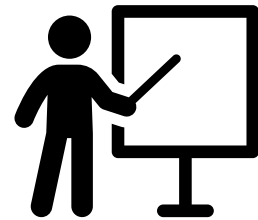
校董會（委派權限予校長，監督風險管理及危機應變計劃的實施）



校長及副校長（實施資訊保安政策，對敏感資料進行分類，監督其傳輸及儲存安全）



IT主管（設計學校伺服器安全指引及帳戶管理政策，制定資料外洩處理流程）



IT 技術員（根據指引確保敏感資料僅限授權人員存取，執行伺服器及網絡設備的日常維護）



教師+學生（遵守學校的資訊保安指引及程序）

學校資料安全中的 責任區分

學校常見個人資料



01 學生健康資料

02 學習成績及評估資料

05 閉路電視資料

03 教師人事資料

04 家長聯絡及財務資料

05 學校活動照片及紀錄



個人資料儲存方式

考慮資料特性而決定儲存方式

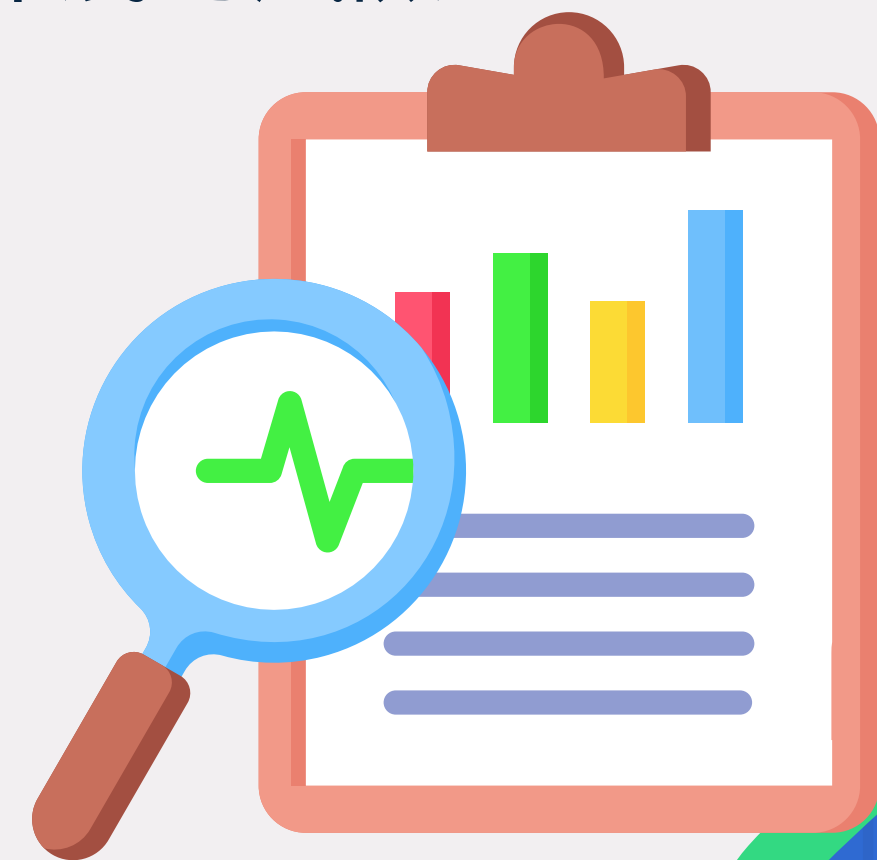
- 公開雲
- 私有雲
- 內聯網
- 離線主機
- 移動儲存裝置
- 紙本



減少資料外洩

教職員在外出工作期間，要留意使用以下的裝置，減低資料外洩的風險

- 個人電腦
- 手機
- 手機內的帳戶
- 移動儲存裝置
- 公用電腦



展示學生相關資料



香港科技大學
THE HONG KONG
UNIVERSITY OF SCIENCE
AND TECHNOLOGY

工學院院長辦公室
OFFICE OF THE DEAN OF ENGINEERING

HKUST Rankings in Engineering
• No. 1 in Hong Kong *
• No. 33 in the World *

8 December 2024

Mr Chu Ka Tim
Principal
Shatin Pui Ying College
9 Fung Shun Street
Wo Che Estate
Shatin
New Territories

Dear Principal,

RE: Recognition of the Student's Excellent Academic Achievement

We are very pleased to inform you that [redacted] and [redacted] from your school have been awarded the HKUST Dean of Engineering Scholarship. It is established to recognize outstanding academic attainments at the HKDSE Examinations. The HKUST School of Engineering are extremely gratified that we admit excellent student(s) from your School. We would like to take this opportunity to express our heartfelt appreciation to your School for nurturing our next generation.

I have the pleasure in enclosing a Certificate Box for your retention. I would appreciate it very much if you could bring this to the attention of your students, and encourage them to apply to HKUST School of Engineering.

If you have any questions or need any further information, please do not hesitate to contact us (email: sengoutreach@ust.hk; phone: 2358-8988), or visit our website at <https://seng.hkust.edu.hk>.

We look forward to receiving more students from your School in the coming years. Let's join hands in grooming future Engineering leaders.

Yours sincerely,

Professor Yu-Hsing WANG
Associate Dean of Engineering (Undergraduate Studies)
Professor of Civil and Environmental Engineering

學校經常展示學生升學等資料, 一方面作表揚之用, 另一方面亦收宣傳之效

不過, 這個安排本意是好, 但仍需徵得學生及家長同意



學校網頁

學校網頁應否公開獲獎學生個人資料？

學校網頁應否公開老師的姓名？

如果需要公佈學生分班名單，是否應以其它方式如內聯網等公佈？





涉及個人資料的課外活動

老師經常帶學生參加其它機構舉辦的課外活動，老師應否提供學生名單？如課外活動涉及錄影，老師又應當如何處理？



任天堂(香港)有限公司
Nintendo (Hong Kong) Limited

香港九龍紅磡都會道 10 號都會大廈 2103-07 室
UNIT 2103-7 THE METROPOLIS TOWER,
10 METROPOLIS DRIVE,
HUNG HOM, KOWLOON, HONG KONG.
TEL: 3167 7839 FAX: 3167 7840

拍攝同意書

致 任天堂(香港)有限公司

本人（參加者姓名（請填寫中文全名）：_____）已閱讀及同意本拍攝同意書的條款及細則，現附上同意書以作證明。

條款及細則：

• 任天堂(香港)有限公司（下稱「任天堂」）將會拍攝 2024 年 10 月 19 日至 20 日於東港城（將軍澳重華路 8 號）舉辦的《瑪利歐賽車 8 豪華版》及《斯普拉遁 3》比賽（下稱「本次活動」）的情況，部份賽事將有機會在 YouTube、Facebook、Instagram、官方網頁及社交媒體等平台（包括任天堂母公司及旗下所有子公司的平台，下稱「平台」）進行網路直播時播出，並無限期公開所有記錄。



Future GEN GIRLS
明日女菁

收集個人資料聲明

1. 收集目的

您提供的個人資料將被處理以用於以下目的：

- 參加峰會和峰會附帶事項（包括核實參加者是否同意參加峰會，與法定監護人或參加者溝通以參加峰會）
- 審計
- 推廣峰會和基金會
- 推廣基金會及其 / 夥伴 / 支持機構和贊助商開展的公益活動
- 個人資料的提供屬自願性質。如果個人資料不足，基金會可能會拒絕獲邀學生的參加峰會申請。

2. 個人資料的種類

可能處理的個人資料類型包括：

- 姓名
- 聯絡電話
- 電郵地址
- 就讀學校和班級

• 父母及 / 或監護人的姓名及其與參加者的關係及其聯絡電話

收集學校表格數據

最小化資料收集（避免不必要的身份證號碼）
制定保存個人資料時期



Part II Parent / Guardian Data 家長或監護人個人資料 (*中、英文姓名, 請依身份證抄寫)

Parent/ Guardian Name in English (Note 2) 家長/ 監護人英文姓名		Parent/ Guardian Name in Chinese (Note 2) 家長/ 監護人中文姓名	
)	Relation 關係	Occupation 職業	
	Home Tel. No. 住宅電話	Emergency Tel. No. 緊急聯絡電話	
地址與學生相同) ☐		Different from student (地址與學生不同)	

是否有必要收集
家長個人資料??

有關「學校個人資料私隱政策」及收集學生／家長或監護人個人資料事宜

沙田培英中學

敬啟者：

有關「使用家長及學生的相片、錄像、作品」事宜

本校為讓學生發展多方面的才能，致力推行多元化學習及大型活動，在舉辦各類型活動及學習過程中，會進行拍照、攝錄或展示學生創作的作品，好讓家長及公眾人士透過學校網頁、學校刊物、宣傳品、展板及講座等途徑認識及嘉許同學之努力與表現。現希望取得家長支持，並同意學校使用家長及學生的相片、錄像、作品於教育及推廣等用途上。

如 貴家長不同意學校使用家長及學生的相片、錄像、作品在教育及推廣等用途上，請於 9 月 13 日或之前以書面形式通知學校。當日後有 貴子弟的肖像出現在團體活動照片或活動時，校方會遮蓋 貴子弟的樣貌。家長日後如改變意向，也可隨時以書面形式通知學校。如對上述事宜有任何查詢，請致電 2691 7217 與本校職員聯絡。

此致
貴家長

校長

朱嘉添

謹啟

二零二四年九月二日



制定資料外洩處理流程

學校應事先制定簡單流程，當事故發生後可啟動緊急應變小組
(如IT組+行政主任+副校長)第一時間應對



**斷開相關
設備網絡
連接**



**通知政府有
關部門**



**確定資料
外洩範圍**



**提供透明信息
以減少恐慌**

不一定所有資料外洩事故都
在數碼世界發生



私隱專員公署回應多宗學校資料外洩事故 (2024年10月發布)

2024年上半年，香港多間中學報告學生個人資料外洩事件。其中一宗典型案例發生於一間位於九龍的中學（匿名以保護隱私，PCPD調查中），約500名中一至中六學生的資料（包括姓名、身份證號碼、電話號碼及家長聯絡資訊）因伺服器遭受釣魚攻擊而外洩。攻擊者透過偽造的校長電郵誘導IT技術員點擊惡意連結，導致系統漏洞暴露。學校於事件發生後三日內通報PCPD，並通知受影響家長。總受影響人數約1,200人（包括家長），無證據顯示資料已被濫用，但調查顯示類似事件在2024年影響了至少五間中學，累計外洩資料逾2,000份。

個人資料私隱專員鍾麗玲指，私隱專員公署在去年共接獲157宗資料外洩事故通報，當中涉學校及非牟利機構的個案共61宗，較前年的25宗升近一倍半（140%）；今年首三季亦已接獲51宗，預計今年全年數字會有升幅。

年份	學校及非牟利機構的資料外洩事故通報宗數（佔整體個案的百分比）	資料外洩事故通報總數
2022	25（約24%）	105
2023	61（約39%）	157
2024（截至9月）	51（約33%）	155

資料來源: 信報: 學校及NGO資料外洩事故呈上升趨勢，私隱署今年首三季接51宗
<https://news.hket.com/article/3845554/%E8%B3%87%E6%96%99%E5%A4%96%E6%B4%A9%EF%BD%9C%E5%AD%B8%E6%A0%A1%E5%8F%8A%8D%E6%B4%A9%E4%BA%8B%E6%95%85%E5%91%88%E4%B8%8A%E5%8D%87%E8%B6%A8%E5%8B%A2%E3%80%80%E7%A7%81%E9%9A%B1%E7%BD%B2%E4%BB%8A%E5%B9%B4%E9%A6%96%E4%B8%89%E5%AD%A3%E6%8E%A551%E5%AE%97>



硬件防護

1. 定期更新防火牆軟體版本，並進行漏洞掃描測試
2. DMZ 應隔離公開服務（如學校網站檔案伺服器），防止攻擊滲透主網絡
3. 學校 IT 主管應每年進行風險評估，特別針對儲存學生資料的伺服器



學校伺服器安全指引



負責資料保安的IT主管及技術員必須注意:

01

每月/季度進行關鍵保安修補

03

啟用帳戶多重認證(MFA)功能

02

定期覆檢敏感資料存取權限

04

刪除不必要的帳戶 (如離職員工)

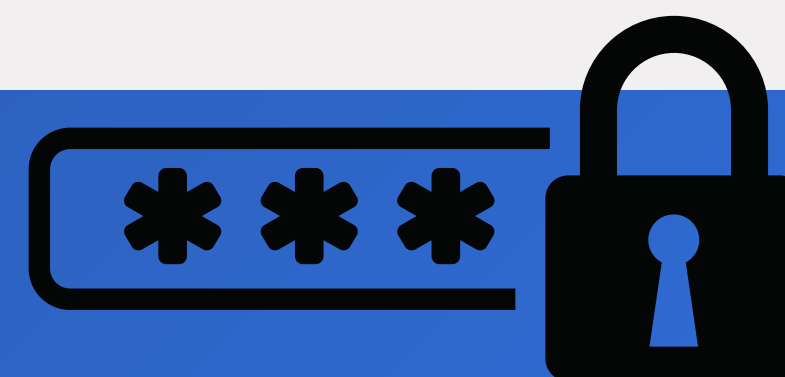


帳戶管理政策 - 存取權限與密碼

誰人擁有甚麼存取權限？誰人擁有最高權限？

密碼是否需要定期更換？是否需要使用複雜的密碼組合？

已離職同事的戶口應如何處理？





閉路電視資料



安裝閉路
電視監察
系統的目
的



誰人可翻
查校園的
閉路電視
片段



制定閉路
電視監察
政策



為負責閉
路電視的
職員制定
工作指引

參考 PCPD 《閉路電視監察及無人機使用指引》，學校應進行私隱影響評估，確保不侵犯學生私隱



保祿六世書院 閉路電視 (CCTV) 使用檢查清單

- 條例合規:
 - ☐ 確定閉路電視系統是否具有錄影功能 (照片或錄像)。如沒有，則通常不受條例規管。
- 必要性評估:
 - ☐ 使用閉路電視對資料使用者履行其合法職能及活動是否合理。
 - ☐ 是否有其他隱私侵犯程度較低的方法。
 - ☐ 決定使用閉路電視是否有迫切性 (例如有關使用是基於公眾利益或公眾安全)。
 - ☐ 確定使用閉路電視的特定目的，及清楚界定要處理的問題。
 - ☐ 收集相關資料，以決定閉路電視是否可以有效地解決當前的問題。
 - ☐ 評估使用高解像設備攝錄個人的仔細容貌，是否真正有需要。
 - ☐ 如閉路電視附帶有任何面部識別功能時，確定是否有強而有力的理據。
 - ☐ 諮詢可能受閉路電視影響的人士，了解他們有甚麼關注。
 - ☐ 在沒有充分的理據下，不應採用隱藏式的閉路電視進行監察。
 - ☐ 清楚釐定監察的範圍和程度。
- 攝錄機及告示:
 - ☐ 閉路電視攝錄機的設置不應不必要地侵犯個人的私隱。
 - ☐ 在人們預期有私隱的地方 (例如更衣室) 不應安裝閉路電視攝錄機。
 - ☐ 應妥善保護整個閉路電視系統，避免遭人故意破壞或非法查閱。
 - ☐ 在受監察範圍的入口和範圍內張貼明顯的告示。
 - ☐ 告示應包括閉路電視系統操作者的資料、監察的特定目的，以及負責處理個人資料私隱問題的人士的聯絡資料。
- 妥善處理攝錄影像:
 - ☐ 在達到收集個人資料的目的後，應盡快從閉路電視系統刪除所收集的資料。

識別及應對釣魚郵件與詐騙行為

老師們，請問：

- ▶ 您有否遇到過涉及學生個人資料外洩的釣魚郵件案例？
- ▶ 您是否了解釣魚防範步驟？
- ▶ 學生敏感資料是否安全儲存在雲端？
- ▶ 您會否在多個平台使用相同密碼



釣魚郵件案例

案例：騙徒以校長名義發出的電郵，要求教師回覆

結果：兩位教師未能識別此為釣魚郵件而進行了回覆。學校為了保障資料安全，迅速對所有系統進行全面的安全檢查，並立即向警方報告了此次事件。





教職員數據保護意識



利在教職員會議中強調老師保護學校數據的重要性和責任

在學校公告板上張貼數據保護的信息

透過預先宣布學校將進行釣魚郵件模擬測試，以評估並提高教職員的警覺性



留意個人電郵有否不尋常的登入記錄



收到不明來歷短訊或電郵時要提高警覺



切勿隨意打開短訊或電郵的附件、連結

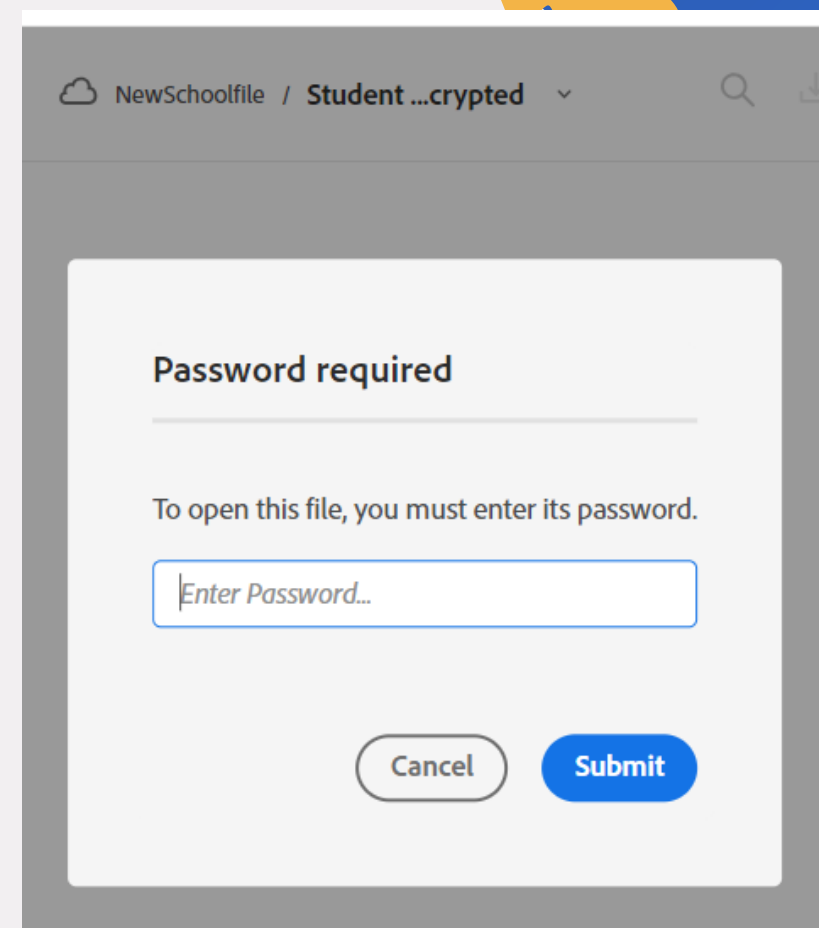


對網絡釣魚及其他詐騙行為提高警覺



如何保護雲端數據？

必須加密學生敏感資料如 Special Education Needs (SEN) 狀況或健康狀況

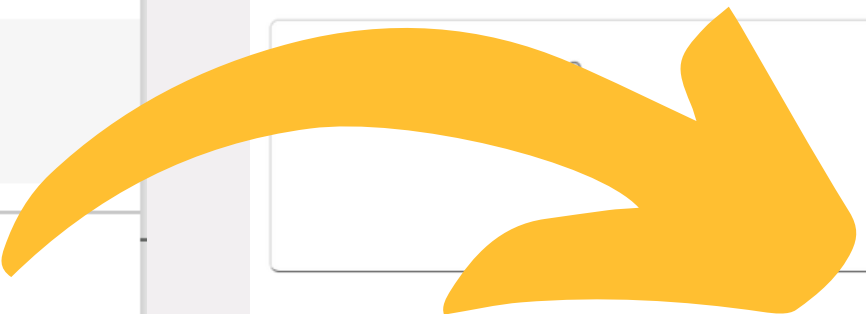


學校應實施雲端數據自動備份策略，把校政文件、教學文件及學生文件定期備份，以減低攻擊後的影響

雲端分享權限的風險



☒	Restricted
☐	Pope Paul VI College
☐	Anyone with the link



Share "(Teacher) G... Class).pdf" ... ? x

👤 Add a name, group, or email ✎

CCCCO

🔗 Copy link ⚙️ ➤ Send

分享權限須逐檔審核，
避免全機構分享。

必須檢查是否有機會分享給全個機構

學生資訊素養

提升學生辨別釣魚網站或詐騙電郵的特徵

講解電郵騙案的騙案的各種手法，提高學生安全使用電郵的意識及正確的態度



Search without being tracked



Switch to DuckDuckGo. It's private and free



Make DuckDuckGo your default search engine.

[Set As Default Search](#)

BEST PRIVACY



Get our free browser for even more privacy.

[Download Browser](#)

教導學生使用 duckduckgo 和其它 Search Engine 之區別，加強學生意識

反思問題

- 學校是否備有數據外洩應變計劃？
- 學校是否已實施帳戶存取權限審核？
- 最近一次伺服器及網絡安全審核何時進行？
- 教職員是否熟悉網絡釣魚攻擊手法？
- 雲端分享權限是否定期審核？
- 閉路電視政策是否已制定？
- 學生是否接受數據安全教育？



保護數據不是選擇，而是責任

全校合作，確保資料安全

