香港紅卍字會大埔卍慈中學

保障個人資料私隱指引

2026 年 2 月

香港紅卍字會大埔卍慈中學

保障個人資料私隱指引

引言：《個人資料（私隱）條例》

《個人資料（私隱）條例》由一九九六年十二月二十日起實施，目的是在個人資料方面保障在世人士的私隱。條例適用於任何直接或間接與一名在世人士(資料當事人)有關的資料、可切實用以確定有關人士身分的資料，以及其存在形式令查閱及處理均是切實可行的資料。條例亦適用於任何控制個人資料的收集、持有、處理或使用的人士(資料使用者)。

條例簡介

個人資料(私隱)條例載列六項保障資料原則，包括資料使用者在收集、準確性、使用、個人資料保障、透明度、查閱及更改個人資料各方面，必須遵從該六項原則的規定。

制定及提供個人資料(私隱)的政策

所有教職員處理可供辨認的個人資料時務須提高警惕，應按照《個人資料(私隱)條例》(第 486 章)的規定，實施有關收集、使用、保障和查閱資料的政策及措施，確保個人資料受到保障。

保障資料第 1 原則:收集資料的目的及方式

學校當循合法及公平的方式收集學生個人資料；而收集資料的目的，是處理學生申請、學生紀錄、舊生或由學校代表進行的聯繫及通訊活動事宜。持有學生紀錄的用途包括作為與學生聯繫及通訊活動有關的聯絡、回覆及跟進行動之用、傳訊及校友活動。學生向校方所提供的個人資料，純屬自願。

保障資料第 2 原則:個人資料的準確性

請學生/家長確保所提供的資料正確無誤。學生如對所提交的個人資料有任何查詢，或對所提供的資料有任何更改，請與校務處聯絡。

保障資料第 3 原則:個人資料的使用及接受資料披露人士類別

學生及家長所提供的個人資料，會供學校在工作上有需要知道該等資料的職員使用(例如心理學家)。除此之外，學校職員在需要時亦只會向下列有關方面披露該等資料：

(a) 其他涉及評估學生的申請或向學生提供援助的有關方面，例如教育局、社會福利署等；或
(b) 學生/家長同意向其披露資料的人士/機構；或
(c) 由法律授權或法律規定須向其披露資料的人士/機構。

在上述情況下，該等人士亦只可將學生資料用於指定目的上，即必須與學生申請或接受服務或援助有關連。

保障資料第 4 原則:個人資料保障

學校對學生及家長所提供的個人資料必須絕對保密。除非預先獲得學生及家長的同意，否則有關資料(包括公開及轉移的資料)只可用於收集該等資料時所述明的目的或與其直接有關的目的，或是條例所容許的目的上。
學校必定採取所有切實可行的安排，以確保所持有的資料受到保障而不受未獲准許的或意外的查閱、處理、刪除或其他使用所影響(儲存資料的地點、儲存設備的保安措施及查閱資料人士的操守)。學生個人資料的保存時間，將不會超過收集該等資料的目的所需時間。

保障資料第 5 原則:透明度

學校在收集學生及家長的個人資料時，會清楚說明收集目的；除非事先獲得學生及家長的同意，否則所收集的資料（包括公開或轉移的資料）僅會用於該等明確說明的目的、與其直接相關的用途，或《個人資料（私隱）條例》所允許的其他用途。

保障資料第 6 原則:查閱及改正個人資料

除了《個人資料(私隱)條例》規定的豁免範圍之內，學生/家長有權就學校備存有關學生的資料提出查閱及改正要求，但並不包括已達成使用的目的後而刪除的個人資料。學生的查閱權利包括在繳付所需費用後，取得學生要求的個人資料的複本一份。查閱或改正資料要求應以書面提出(收到書面申請時要蓋上日期)，學校會於收到學生/家長查閱資料要求申請表後四十天內回覆。根據《個人資料(私隱)條例》，在下述情況下，學校有可能拒絕接受學生改正資料的要求，並將拒絕查閱及改正資料的原因，記錄在**學校備存的記錄簿**，拒絕查閱及改正資料的詳情如下：

(a) 要求不是以書面提出；
(b) 學校有理由相信所持有的個人資料並非不準確；
(c) 學校不獲提供充分資訊，以確定學校所持有的個人資料並不準確；
(d) 學校有理由不信納該項要求所提出的改正是準確的；或
(e) 有另一資料使用者控制該等資料的使用，而控制的方式禁止校方依從該項要求，則校方會通知學生關於該資料使用者的地址及姓名或名稱。

參考資料：

1. 香港法例第 486 章：《個人資料(私隱)條例》。

附錄：資料外洩事故處理及通報指引

一. 引言

本附錄旨在補充學校現有的《保障個人資料私隱指引》，為校方在面對懷疑或已證實的個人資料外洩事故時，提供清晰的應變程序及通報機制。本指引參考香港個人資料私隱專員公署（下稱「公署」）之建議編制。

二. 定義

資料外洩事故是指學校持有的個人資料（如學生、家長、教職員、校友的資料）懷疑或已經遭到外洩，導致資料面臨被未獲准許或意外的查閱、處理、刪除、喪失或使用的風險。

常見例子包括：

- 遺失載有學生資料的 USB 手指、手提電腦或實體文件（如試卷、報名表）
- 誤將載有個人資料的電郵發送給錯誤的收件人（例如錯誤發送予其他家長）
- 學校電腦系統或內聯網遭黑客入侵或勒索軟件攻擊
- 未經授權的職員查閱敏感資料（如特殊教育需要(SEN)紀錄）
- 獲授予有效查閱權的職員故意地、意外地不當處理個人資料，導致資料外洩
- 不當棄置未經銷毀的紙本文件
- 在電腦安裝檔案分享軟件而導致資料外洩

三. 資料外洩事故專責應變小組

一旦發生資料外洩事故，學校應成立「資料外洩事故專責應變小組」(下稱「應變小組」) 以統籌處理。

成員建議：校長、副校長、訓輔主任、電子教學組統籌（如涉及電子資料)、相關部門主管。

職責：評估風險、制定遏止措施、決定通報對象及後續檢討。

四. 事故處理程序（五步曲）

步驟 1：立即收集資料及通報

發現者責任：任何教職員一旦發現或懷疑發生資料外洩，必須立即向應變小組或校務處報告。

初步資料收集：應變小組需迅速掌握以下資訊：

- 事故發生的時間及地點
- 外洩的資料種類（例如：姓名、身分證號碼、聯絡電話、SEN 資料、財務資料等）
- 受影響人士的估計數目
- 事故起因（例如：黑客攻擊、人為疏忽、盜竊）

步驟 2：遏止事件擴大

學校需立即採取行動減低損害：

- 電子資料：立即中斷受影響系統的網絡連接、更改密碼、遙距刪除遺失裝置內的資料、聯絡互聯網供應商移除網上緩存連結
- 實體資料：盡力尋回遺失物品、聯絡外洩/誤收文件者要求銷毀或退還文件
- 其他：如涉及盜竊或刑事成分，應考慮報警處理

步驟 3：評估損害

應變小組需評估事故對資料當事人（學生/家長/職員）可能造成的傷害程度，以決定通報的必要性。

高風險因素：

- 涉及敏感資料（如身分證號碼、健康紀錄、特殊教育需要紀錄、成績表）
- 資料未經加密處理
- 可能導致身分盜竊、財務損失或人身安全受威脅

步驟 4：考慮作出資料外洩通報

根據風險評估結果，決定是否及何時作出通報。

通報私隱專員公署：

如事故相當可能對受影響人士構成實質傷害，學校應在切實可行的情況下盡快向公署作出通報（使用公署指定的「資料外洩事故通報表格」）。

通報受影響人士（家長/學生/職員）：

如通報能讓當事人採取防範措施（例如更改密碼、留意可疑交易），學校應盡快透過學校通告、電郵或電話通知受影響人士。通報內容應包括：

- 事件簡述
- 涉及的資料種類
- 學校已採取的補救措施
- 對當事人的建議（如何自我保護）
- 通報其他機構： 視乎情況通知教育局、警方或相關服務機構

步驟 5：記錄及檢討

記錄：無論是否對外通報，學校必須完整記錄每宗事故的詳情、調查結果及所採取的行動，以備日後查核。

檢討（防範未然）：事故處理完畢後，應變小組須進行檢討，找出保安漏洞，並修訂相關政策或加強員工培訓，防止同類事件再次發生。

五. 預防措施與員工責任

所有教職員應遵守「員生個人資料及資訊科技處理及保安指引」內列明的原則。相關指引已記載於教師手冊 – 電子教學組的文件內。