jamf

教育合規入門指南

如何建立一套保護學生、教師與社群的國民及學前教育合規計畫

現代國民及學前教育合規環境

在任何產業中，裝置與網路安全合規性可能都是一頭複雜難解的野獸。隨著裝置功能擴展，以及法律與最佳實務不斷更新調整，產業標準也隨之改變。

國民及學前教育環境更加劇了這些複雜性。

探索：

- **如何跟上日新月異的教育合規性規定**
- **以策略性作法規劃合規基礎結構為何至關重要**
- **如何建立可持續的合規實務**

本文件僅供參考，並不構成法律建議。合規性規定依司法管轄區與教育機構而異。學校與學區應諮詢合格的法律顧問，以確定應承擔的具體合規義務。

國民及學前教育的獨特合規挑戰

如同企業的對應單位，學校也須保護連接至學校網路的各式裝置與使用者，並防範網路攻擊。

不同於企業環境，學校必須與家長及大眾維持高度開放且簡便的溝通模式—而這些對象所使用的裝置，皆非貴學區所能控管。

這會形成一個寬廣且脆弱的攻擊面。再加上多數學校與學區均面臨的預算限制，不難理解為何資安合規始終是一項挑戰。

學校裝置與網路使用者也具有獨特性。

企業與學校之間最明顯的差異在於：學校服務的使用者類型極為多元，包括教師與行政人員、學校與學區職員，或許還有最具挑戰性的—兒童。

兒童充滿好奇心。兒童需要具吸引力和互動性的學習工具。他們需要養成盡責數位公民所需的技能，並能與教師、家庭與同儕分享所學。

兒童的好奇心無窮無盡。

因此，學校 IT 人員須為他們設置適當的邊界。他們的任務是：在不拖慢日常教學的前提下，保護兒童免於網路釣魚攻擊、惡意軟體以及危險或不當內容。

此外，學校還必須在網路安全實務與學生隱私權的顧慮之間取得平衡。而對於部分高風險弱勢學生（如 LGBTQIA + 學童），隱私遭到侵犯可能對其心理健康與人身安全造成極大風險。

各種標準與規定交錯

全球各地的教育環境正面臨來自多方的密切審查與巨大壓力：

1. **國家與國際法規**
2. **地區法令與標準**
3. **教育監管機構**

例如，在歐盟，《一般資料保護規則》（GDPR）用以保護學生資料；英國則有《英國一般資料保護規則》（UK GDPR）與《2018 年資料保護法》。另有兒童專屬的法令和法規，例如美國的《兒童網路保護法》。

除此之外，學校也常須遵守其他可能影響資料、網路與裝置安全的規定，例如美國的《美國身心障礙者法案》。

亦不可忽視負責安全合規等級認證的體系，例如 StateRAMP 與 FedRAMP；這兩者是政府單位在雙方往來時，常要求學校達到的安全標準。

數位轉型的挑戰

由於 COVID-19 疫情及各界對校園安全的關注急遽攀升，全球國民及學前教育的課堂幾乎在一夕之間發生巨大轉變。

正在數位轉型的學校會做出以下改變：

- **從紙本學習轉向數位學習環境**
- **須遵循更多資料收集與儲存規定**
- **導入遠距或混合式學習，並考量其對合規性的影響**

各架構間共通的合規性主題

除了學校與學區在合規性方面與其企業對應單位的無數差異外，
學校也必須遵循以下規定與最佳實務：

- 資料保護與隱私
- 裝置與網路安全
- 存取控制與身分認證
- 事件回應與外洩通知
- 稽核軌跡與報告

國民及學前教育的網路攻擊日益普遍

遺憾的是，學校與學區對網路犯罪者極具吸引力。

學校所持有的資料（包括社會安全號碼和其他身分識別碼）具有高度價值。
此外，部分學區還會留存家長的信用卡資訊（用於營養午費或學雜費），成為犯罪者快速獲利的目標。

這種現象相當普遍，英國的《2025 網路安全漏洞調查》即顯示，44% 的小學與 60% 的中學在該年度曾發生資安事件或攻擊。

未合規的代價

許多學校與學區已付出此代價。有些被迫支付贖金，有些因資料外洩遭家長提告，也有些因無力保護其網路和資料，或未妥善通報外洩而成為頭條新聞。

財務處罰與法律後果

如上所述，學校、學區，甚或供應商若未能遵守嚴格的安全合規與資料保護政策，往往會面臨財務與法律麻煩。

例如支付高額贖金、違反聯邦或國際學生隱私法，或遭家長提告。

供應商遭攻擊的近期案例

2024 年，某套廣為使用的學生資訊系統（SIS）與教育科技平台，因遭駭客威脅若不支付贖金即公開學生資料，最終支付了 285 萬美元贖金。

隔年，該名駭客又以相同要求，向使用該套軟體的各個學區進行勒索。

聲譽受損與社群信任

學校可能因此失去大量資助者、家長與在地企業等社群成員的信任，未明確規範如何告知社會大眾外洩情事時尤然。

學區遭攻擊的近期案例

2023 年，美國某都會學區遭勒索軟體攻擊後，並未向大眾說明，駭客當時曾索要贖金，並揚言若未如數支付，將公開極度敏感的資料。該學區拒付贖金後，相關資料遭公開。即便事發後，該學區仍遲遲數月，才通知受影響的個別學生。最終引發眾怒並損害該學區的聲譽。

家長對於學生隱私權向來高度重視，若缺乏明確的作業準則，學校與學區在接獲各方不同甚至矛盾的意見時，極易陷入作業混亂的局面。若校方處理方式前後不一，大眾往往會產生最壞的聯想。

運作中斷與資源分配

網路攻擊的最終目的或許是獲利，但其手段可能在諸多方面中斷學校體系運作，導致：

- **薪資發放延遲**
- **成績報告延誤**
- **學校被迫停課數日**

學校停課的近期案例

2026 年 1 月，英國一所中學即因網路攻擊而完全停課一週。這次攻擊導致「該校 IT 系統全面癱瘓，包括電話、電子郵件、Google Classroom、校務管理系統及 Microsoft SharePoint。」

在了解上述各項風險後，接下來我們將探討建置完善合規計畫的核心基礎要素。

國民及學前教育
合規的四大核心支柱

1. 學生資料隱私權

什麼是學生資料？

制定資料保護政策和程序的第一步是了解哪些內容屬於學生（甚或教師或家長）資料。這些資料包含但不限於：

- 姓名、生日、住址與個人電子郵件地址
- 家長姓名、職場資訊與信用卡號
- 考試分數與成績等學習資料
- 健康、行為與出缺勤紀錄

資料最少化原則

盡可能減少您收集的資料量，並盡量縮短資料保存時間，便能大大保護學生資料隱私。只收集執行必要功能所需的資料、僅在必要期限內保存。駭客便無法存取您沒有的資訊！

僅授權實際有需求者，存取其職務所需的特定資料。
透過限制存取權限，可有效縮小資安攻擊面。

制定同意與通知規定。傳達您要蒐集什麼資料及蒐集理由，以及儲存位置與保存期限時，務必透明公開。這會大大促進社群信任。

全面管理第三方供應商，例如測驗或教育軟體公司。確認其是否符合安全與隱私規範要求。建立政策與工作流程，明確掌握其可存取的資料內容、用途及後續處理方式。如此就能防範最常見的攻擊類型，即第三方資料外洩。

國民及學前教育合規的四大核心支柱

2. 存取管理須知

基於角色的存取原則

如前所述，管理網路與資料存取權的核心原則為「最小權限原則」—僅授予使用者完成其職務所需的存取權限，無過度授權。請自問：誰該在何時存取哪些資料？

實施基於角色的存取權

確保您具備一套控管機制，能在適當時間與情境下提供教職員所需的權限，同時也能以安全方式將訪客存取權限制在最低範圍內。若將此類權限與學生、家長及教師的身分識別編號綁定，控管效果通常最為理想。

基於年齡的靈活彈性

請牢記在心，存取與認證規定既因角色而異，也因年齡而異。年幼學生可能無法記住複雜密碼，而年長學生則可以。此外，隨著學生年歲漸長，他們的存取權理當依課程內容而變。依年級或年齡指派角色給學生，便能大幅減輕您長期管理的負荷。

國民及學前教育合規的四大核心支柱

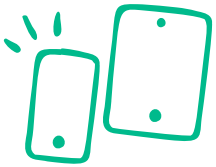
3.

資安基礎結構規定

訂定明確的資安基礎建置規範，並採行嚴謹的端點防護策略，往往是區分「局部資安外洩」與「全面外洩」、「裝置遭入侵」與「裝置維持安全」的關鍵。

端點防護策略

確保端點防護具備以下功能：



- 自動化威脅防護與修復
- 裝置上分析與主動通報
- 資料政策自動化落實

與這些功能本身同等重要的是，導入解決方案時，不得損及資安、隱私權與系統效能。

考慮網路分段

防止局部資安外洩擴散至全學區的最佳方法之一，是依據網路使用者身分，或是網路所服務的組織單位，進行網路分段規劃。例如可劃分為：行政和教師網路、學生網路與訪客網路。

續.....

國民及學前教育合規的四大核心支柱

3. 資安基礎結構規定

加密標準與導入

應詳細檢視各主管機關所訂定的加密與導入實作策略，
以及自身可落地執行的相關最佳實務，包括：

- 高強度加密演算法
- 安全金鑰管理
- 靜態與傳輸中的資料加密

定期資安評估

隨著學生結構變動與教育科技工具持續迭代，學校須訂定定期的資安評估計畫。此項資安維護工作是學校維持持續合規的必要環節。

這也讓您有機會：

- 納入新興技術
- 訂定對應政策，以因應內外部合規要求與最佳實務的各項調整變動
- 檢查是否有任何漏報處或新的報告需求
- 評估合作供應商，及其是否能滿足學校的新增或擴充需求

國民及學前教育合規的四大核心支柱

4. 文件化與稽核準備

為稽核做準備看似繁瑣，但長遠看來，妥善的稽核準備不僅能在需要稽核時節省您的時間，也能確保您的網路和資料更加安全。

以下是準備方式：

應管理與報告的關鍵資料類型

請牢記您須追蹤的三大類資料：

學生資料：出缺勤、成績、操行成績
運作資料：IT 資產報告、網路設定、資安日誌
法規資料：合規文件、供應商合約、稽核報告

紀錄保存的關鍵實務

確保您的資料維持安全、集中化管理且合規。主要作法包括：

- 使用學生資訊系統（SIS）
- 管理軟硬體資產
- 視情況將紀錄進行數位化

續.....

國民及學前教育合規的四大核心支柱

4. 文件化與稽核準備

自動化記錄與監控

若您已建立自動收集、分析並即時處置資安日誌資料的機制，稽核作業將更為順暢。不僅可隨時掌握最新清單，也能主動辨識資安威脅，並在威脅變成全面攻擊前加以解決。

事件文件化程序

為避免在校內外引發信任危機，學校應事先訂定資安事件的文件化處理程序—預期此類事件必然會發生。確保您已建立記錄和簡報程序：

- 事件之清晰且依時間先後的說明紀錄，以及用來處理該事件的工具
- 安全、運作與財務影響評估
- 指令輸出、日誌檔案與受影響系統的報告

定期合規性審查

一如定期資安評估，審查同樣不可或缺。合規工具和規定隨時變動，最佳實務亦然。投入時間與人力定期進行合規性審查，有助於避免法律處罰、罰款以及長期的聲譽損害。

合規準備度評估

您準備好了嗎？

自我評估檢查清單

此一持續演進、標準嚴格且作業複雜的合規流程，往往容易讓人望而生畏。檢查清單為相當實用的準備工具，可協助團隊避免遺漏任何合規作業細節。

技術基礎結構準備度

您是否已建置完成以下項目？

- ☐ 裝置資產清冊與管理系統
- ☐ 集中式身分及存取管理
- ☐ 學生與行政系統間的網路分段
- ☐ 在所有裝置上全面部署端點防護
- ☐ 靜態與傳輸資料加密
- ☐ 自動化備份與復原程序
- ☐ 資安監控與警示功能

政策與治理準備度

您是否已製作相關文件紀錄，或訂定建立以下規範：

- ☐ 完備的可接受使用政策
- ☐ 資料保存與銷毀政策
- ☐ 資安事件回應處置程序
- ☐ 教職員培訓計畫
- ☐ 供應商管理與盡職調查流程
- ☐ 定期政策審查與更新排程

運作準備度

是否已執行以下作業：

- ☐ 指派專責合規人員或專門團隊
- ☐ 定期執行資安評估作業
- ☐ 啟用稽核軌跡追蹤功能
- ☐ 建立資安外洩通報程序
- ☐ 制定家長及學生的溝通規範
- ☐ 啟用文件化與紀錄保存系統

供應商與第三方準備度

您是否已備妥以下項目？

- ☐ 與所有供應商的資料處理協議
- ☐ 資安認證驗證作業流程
- ☐ 定期執行供應商資安評估作業
- ☐ 明確的資料共享與存取權限控管機制
- ☐ 供應商事件通報規定

Jamf for K-12 如何支援合規

雖然 Jamf for K-12 本身無法自動化實現並確保學校符合合規要求，但其可透過以下功能，提供支援學校整體合規策略的必要基礎建置：

裝置管理與安全性

- 集中式裝置註冊與設定
- 資安政策自動化落實
- 遠端裝置管理與防護
- 完整的裝置資產清冊與報告

存取控制與身分認證：

- 與身分識別提供者整合以支援單一登入（SSO）
- 基於角色的存取管理
- 基於角色的 App 與內容存取限制
- 跨裝置與平台的安全認證

可擴展的管理功能：

- 於所有裝置上統一套用合規政策
- 高效管理大規模裝置部署
- 針對大量裝置機群的可擴展政策部署
- 支援多元學習情境（一人一機、共享裝置、BYOD）

整合功能

- 可與學校現有資訊系統相容整合
- 支援第三方教育應用程式
- 整合網路基礎設施
- 連結身分及存取管理解決方案

Jamf 平台可做為基礎建置層，協助學區建置穩定、安全且易於管理的技術環境，滿足各項合規架構的要求。

本平台的自動化功能與各項能力，可讓學校團隊專注於合規政策、培訓工作與策略性合規行動，而非日常裝置管理的各項挑戰。

國民及學前教育領域的合規工作從非一蹴可幾。

而是一項持續優化的過程，會隨著學校的技術設備、學生結構與法規環境持續調整演進。

所幸的是，學校無須獨自建置此一合規基礎。

Jamf for K-12 提供各項工具，協助學校團隊管理裝置、落實合規政策，並維持合規要求所須的安全、可稽核之營運環境。這代表學校可減少投入基礎建置的時間，將更多精力投入至真正具核心價值的工作中。

申請免費試用

jamf