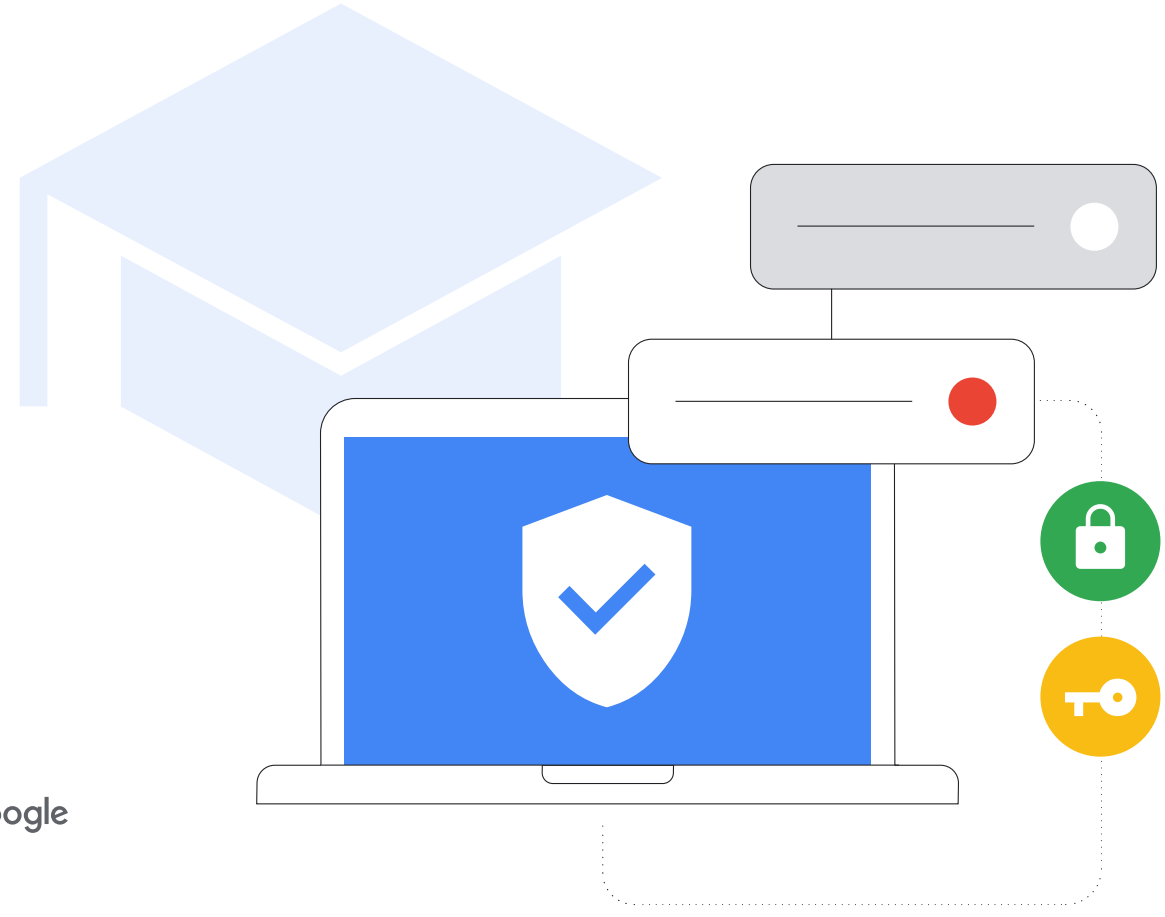
Google for Education

從幼兒園到高中的網路安全指南於

2023 年 8 月更新



Safer with Google

內容提要

美國網路安全暨基礎設施安全局 (CISA) 的《Protecting Our Future》(保護我們的未來)[1] 報告指出，從幼兒園到高中的各級學校皆必須致力加強網路安全，保護學生與他們的家人、教職員和社群。為了強化網路安全，本文將為從幼兒園到高中的各級學校 IT 管理員，提供校內軟硬體的設定指南與最佳做法，其中涵蓋一般最佳做法，以及 Google 產品和服務專用指南。Google 的使命是彙整全球資訊供大眾使用，使人人受惠。Google for Education 團隊也秉持這項重要理念，打造一系列教學與學習工具。本指南將分享我們開發這些工具的經驗。

我們會依主題介紹資安最佳做法，進一步說明相關設定和風險評估策略，並介紹 Google 服務 (尤其是教育工具) 採取的網路安全措施。本文提供的詳細指南適用於所有產品或服務，不過我們相信 Google 產品本身即具備優異的防護功能，因此不需額外設定，就能有效防禦常見攻擊。

風險

教育機構是網路攻擊的主要目標。不肖人士會利用漏洞攻擊資料量龐大的學校環境來牟利。勒索軟體的攻擊手法不斷翻新且難以阻絕，有 46% 的學校機構自覺遲早會遭受波及。其中的 42% 認為，勒索軟體是日益普遍的威脅，最終難免成為其下手目標。2020 年，各校因應局勢改採遠距教學，網路安全漏洞因此大幅增加，也讓駭客有機可乘。

防護措施

網路攻擊雖然層出不窮，但並非讓人束手無策。雖然目前沒有任何技術能夠保證完全消除風險，教育機構和教育科技供應商仍可以合作採行最佳做法，制定安全完善的方法來大幅降低風險。只要採取適當的預防措施和政策來保護使用者、裝置和資料隱私權，教育機構就能妥善管控風險並避免攻擊。

重要建議

- **使用安全的驗證機制**保護機密資訊、電子郵件、檔案和其他內容，並防止未經授權的使用者存取教育系統。盡可能採用高強度密碼、兩步驟驗證、密碼金鑰與密碼管理工具等最佳做法來驗證使用者身分，特別是 IT 管理員和處理機密資訊的教職員。
- **套用合適的安全性設定**來保護使用者、資料和環境。Google 產品均內建強大的防護機制，不過管理員仍需妥善運用及設定網路及系統，以確保安全無虞，並謹守零信任和最低權限原則來保護學校：只讓使用者存取完成工作所需的軟體、資料、應用程式與系統。
- **更新並升級系統，**確保使用者能隨時防範最新威脅。使用新式作業系統 (OS) 和瀏覽器，並確認使用者在所有裝置上使用的軟體均為最新版本 (或經核准的長期穩定版本)，且會自動更新。升級採用 Chromebook 等更安全的解決方案，可有效提升防護力。目前從來沒有人在 ChromeOS 裝置上偵測出任何勒索軟體。
- **使用即時快訊和監控系統**強化安全防護機制，快速防範潛在問題。您可以使用主要協作和通訊軟體 (例如 Google Workspace for Education) 內建的快訊與監控功能，或另外部署安全記錄及監控解決方案。務必全面追蹤學校網路、裝置、應用程式、使用者和資料的活動，並監控帳戶登入、檔案共用和設定變更的情形，以及裝置活動與電子郵件數量 (尤其是潛藏網路釣魚和惡意軟體的郵件)。確保快訊和監控解決方案為最新版本，以便接收有關資安威脅、重大事件和系統變更等相關通知。
- **向教職員和學生提供資安訓練，**說明如何安全地使用裝置和軟體、判斷及回報潛在威脅，並以適當方式共用資料，加強防範常見攻擊。學校或學區可以製作自有訓練教材，搭配可免費取用的現成資料，提供完整工具包讓教職員和學生使用。

1 https://www.cisa.gov/protecting-our-future-cybersecurity-k-12

Google 產品使用者適用的建議：採用 Google Workspace for Education、Chromebook 等 Google 產品，即可強化學校的網路安全，並輕鬆推行本文所述的建議。這些產品組成的全方位解決方案能有效保護使用者隱私，為機構提供頂尖的安全防護機制。

從幼兒園到高中的各級學校均可採用上述策略和後續報告介紹的其他指南，鞏固資安基礎。

Google 在教育領域採取的資安做法

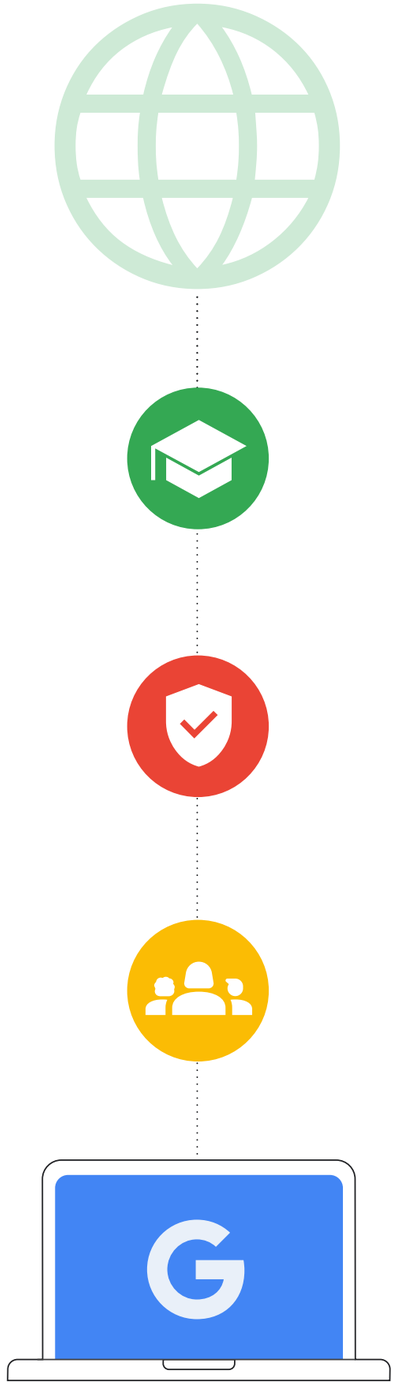
Google 使命是彙整全球資訊供大眾使用，使人人受惠。在教育領域，Google 也秉持這個精神提供服務。因此，Google for Education 團隊致力打造 Chromebook、Google Classroom 等工具，讓學生和老師輕鬆安全地共用及整理自己的內容，並存取與使用各種教育資源和線上工具。

供學校採用的技術應以安全性為出發點、將隱私權納入設計考量、讓學校保有控制權，並提供值得信賴的內容和資訊。Chromebook、Google Workspace for Education 等產品為學校提供符合全球最高教育標準的一流安全防護機制，讓 IT 管理員掌握全盤情況、輕鬆控管資料和安全性政策。這些產品同時也會提供適齡內容，並防範垃圾內容與網路威脅，讓學生在更安全的數位環境中盡情學習。

我們會優先開發產品內建的安全防護功能和控制選項、遵循最高等級的隱私權標準，並提供更多主動式安全防護工具，確保所有人享有安全的學習環境。ChromeOS 裝置可幫助學校防範威脅，也是阻擋勒索軟體的最佳利器，像是 Chromebook 就從未讓這類頭號威脅得逞。

此外，Google Workspace for Education 是全球最熱門雲端式安全通訊和協作套裝組合之一。如要進一步瞭解這兩項產品如何根據本文所述建議保護網路安全，請參閱最後一節。

本報告分為兩個部分：第一部分是從幼兒園到高中的各級學校的一般資安實務指南，適用於所有產品；第二部分則專為使用 Google for Education 產品 (如 Google Workspace for Education 與 Chromebook) 的機構提供設定指南。無論是哪一部分的資訊，都能幫助全校學生及教職員的安全



簡介

從幼兒園到高中的各級學校裝置和網路都很可能會遭受網路攻擊。因此，教育機構必須盡可能採用最強大的安全防護機制來保護學生，防止網路攻擊造成資料、服務、資源、時間及金錢損失。(資料來源)

本指南旨在推廣網路安全最佳做法，協助學校管理員與教育體系保護校園數位環境。從幼兒園到高中的各級學校均可透過這些最佳做法，減輕或避免網路攻擊對教育系統造成的重大危害與經濟損失，並保護學生、他們的家人與教職員。

以學校為目標的網路攻擊日漸頻繁，也越來越嚴重。K-12 Cybersecurity Resource Center (從幼兒園到高中的各級學校網路安全資源中心) 指出，2016 到 2021 年間對外公開的網路事件中，有超過 1,300 起發生於教育機構，範圍遍及美國 50 個州。因此，現今的教學主管必須保護學生和教職員的資料與個人資訊，以及機構的系統和資訊。這項任務十分艱鉅，因為與其他領域相比，教育界在網路安全方面往往更難與時俱進。

勒索軟體、網路釣魚與惡意軟體等網路攻擊一旦得逞，便可能大規模侵害個人識別資訊 (PII)、造成重大經濟損失 (平均贖金金額自 2020 年來已增加 5 倍至 $812,260 美元)，並導致教學與其他校務長期中斷。近期，某間學校的資訊系統便因勒索軟體攻擊全面停擺，不但學生多天無法上學，整個社群都遭到波及。從幼兒園到高中的各級學校資源和資金均有限，如不致力加強網路安全，仍會是勒索軟體的主要攻擊目標。

溝通與合作始終是強化網路安全的最佳做法。我們在編寫本文時參考了具公信力來源的網路安全做法，包括 Google 安全性提示、美國國家標準暨技術研究院 (NIST) 網路安全架構，以及 2023 年 CISA 從幼兒園到高中的網路安全工具包與建議。本文探討 IT 管理員應採取或考量的一般步驟、Google 產品適用的最佳做法和指南，並參考其他公司提供的安全性提示與服務。管理員應根據所用產品，詳閱並採用相關公司的所有最新資安指南，因為這些公司最能說明自家產品的資安最佳做法及過去的各項變更。

按照下列建議採取行動前，請一併考量以下重點：

考量重點：

1. **保護學生：**
   各校需求不盡相同，部分學生可能需要保障安全與隱私權的額外措施。許多教育科技工具會提供依年齡設定資訊存取權的功能，例如限制不當內容，或確保學生的地點和聯絡資料隱私。

2. **您儲存的資料類型：**
   如果您儲存的是機密資料，請務必將資料加密，或存放在獨立位置。

3. **您使用的裝置類型和部署模式：**
   裝置及其中的應用程式必須能自動更新，盡可能提高安全性。同時，您也需要將資料加密並隔離帳戶，確保使用者只能存取自己的資訊。

4. **學校、學區或地方政策**
   學校可能有技術使用相關政策，請務必確認您設定的所有保護措施皆符合政策規定。

Gmail 每天封鎖
1億
個網路釣魚內容

Google 每週識別出
30萬
個不安全的網站。

Google 密碼管理工具每天為
7,400萬
名使用者提供協助。

安全設定檢查每年為
7億
人強化安全保護措施。

一般安全性指南

使用安全的驗證機制

學校及其他機構必須優先建置安全的驗證機制。2022 年第 4 季的資料侵害事件中，有 48% 的入侵管道為安全強度過低/未經認證的帳戶。本節提供的重要建議，可協助您確認使用者的真實身分，並依使用者的角色限制資訊存取權。

IT 管理員應盡可能強制執行兩步驟驗證 (也稱為雙重驗證)，並改用無密碼驗證 (例如密碼金鑰)。如果使用者會從遠端存取教育機構的系統，更應採取這類做法。兩步驟驗證可為線上帳戶多添一道安全保障，讓攻擊者更難入侵。

現今，從幼兒園到高中的各級學校均使用多種裝置與部署模式，技術能力也各自不同。帳戶和裝置安全性機制因使用者角色和類型而異，且有相應的最佳做法：讓 IT 管理員、教職員、高年級學生使用學校配發的裝置，低年級學生則共用學校裝置。以下將討論各個群體適用的建議。

下列幾種驗證方式為適用於多數設定的最佳做法

- **高強度密碼：**
  請使用者在首次登入時自行建立密碼，並嚴格規定密碼長度下限和複雜性需求。使用多個複雜字元組成較長的通關密語，可提高安全性。要求使用者定期變更密碼並非有效做法，因為使用者可能會改用更簡單的密碼或僅做小幅調整，例如只更動一個字元。
- **兩步驟驗證：**
  「兩步驟驗證」是指透過第二個步驟保護帳戶安全，通常透過使用者隨身攜帶的物品完成，例如安全金鑰或可產生一次性驗證碼的手機應用程式。雖然任何形式的兩步驟驗證都可提升帳戶安全性，管理員仍應避免透過簡訊或通話傳送驗證碼，這種方式容易遭受以電話號碼為目標的攻擊。
- **無密碼驗證：**
  密碼金鑰是比密碼更安全、更簡單的替代驗證方法。使用者可透過 PIN 碼、圖案、生物特徵辨識感應器 (例如指紋或臉部辨識)，或輕觸安全金鑰來登入應用程式或網站，不必再費心記住或管理密碼。這些方法不一定適用於每個教育機構，但正逐漸取代傳統的驗證方式，而且更安全迅速。密碼金鑰只能用於使用者註冊的網站和應用程式，因此可幫助使用者防範網路釣魚攻擊。
- **單一登入 (SSO)：**
  採用單一登入，使用者就能以一組憑證存取多個應用程式和網站。使用者只需記住一組憑證，因此較不會寫下來。此外，學校也不必管理多組使用者憑證，進而省下 IT 支援和服務中心相關支出。Google Workspace for Education 本身即支援單一登入，因此使用者可透過自己的 Google 帳戶憑證登入第三方應用程式，或使用其他供應商的憑證登入 Google 帳戶。
- **密碼管理工具：**
  在不使用單一登入的情況下，使用者可透過密碼管理工具，針對學校或公司的各個帳戶與服務，建立不重複的高強度密碼。使用者雖然無法藉由這類工具登入裝置作業系統，但只要登入後，就能管理其他密碼。在任何平台、ChromeOS 裝置和 Android 裝置上的 Chrome，Google 使用者都可使用密碼管理工具。

您可以根據各個群體的年齡、在教育機構內的角色，以及可存取的系統和資料類型，搭配使用特定幾種驗證方法，滿足不同群體的需求。

學校管理員

從幼兒園到高中的各級學校管理員皆負責控管校內系統和大多數資料。從基礎架構、帳戶資料到機構管理的裝置，整個系統安全與否，取決於管理員帳戶的保護措施。因此，管理員帳戶應採用最高標準的驗證方法，包括高強度密碼、兩步驟驗證，以及完善的密碼管理工具。每項方法都能多添一層安全保障，只要搭配使用，管理員帳戶和企業服務皆可獲得最強大的安全防護。

- 管理員應使用實體安全金鑰或需要透過信任的裝置和提示進行的加密式安全兩步驟驗證方法，舉例來說，Google Authenticator 這類服務或是其他會產生一次性驗證碼的應用程式皆可做為這類驗證方法。2019 年之後推出且配備 TPM 晶片的 Chromebook 內建一個電源按鈕，即可用來進行雙重驗證。
- 管理員應使用支援兩步驟驗證且可信任的密碼管理工具，儲存不同服務的密碼。

使用學校配發裝置的教職員

教職員與管理員一樣能存取機密資料，但不負責控管數位基礎架構，技術能力也不盡相同。

- 在法律允許的情況下，使用 Chromebook 的教職員應可選擇透過指紋等生物特徵辨識驗證方法登入。
- 管理員應盡可能強制執行兩步驟驗證，並改用無密碼驗證。如果教職員可從遠端存取教育機構系統，更應採取這類做法。

使用學校配發裝置的高年級學生

(通常為 4 年級以上)

高年級學生接受的資安教育較多，因此更懂得如何保護自己，通常能使用更有力的驗證機制。因此您可以根據他們可能使用的服務類型，採用更具保護力的合適驗證方法。請僅開放高年級學生存取自己的帳戶，以及分享給他們的資訊。

- 使用 Chromebook 的學生應可選擇建立裝置專屬 PIN 碼，加快登入速度。不過對許多學校而言，高年級學生可能還無法或不適合使用生物特徵辨識驗證。
- 請協助每個學生建立不重複的密碼，其中不可包含姓名、班級與生日等個人資訊。務必向學生說明如何設定複雜的通關密語，以及簡單好記的密碼。

共用學校裝置的低年級學生

(通常為幼兒園到 3 年級)

低年級學生仍在學習如何使用教育科技，因此最合適的做法是讓他們存取有限的服務和資料，並搭配簡單的驗證方法。

- 如果學校為低年級或無法使用密碼登入的學生提供第三方密碼替代方案，例如 QR code 或圖案登入，請務必採取預防措施加強防護，因為這些方案的安全性較低。此外，只要驗證碼遺失或外流，管理員就必須修改學生的密碼並更新驗證碼。
- 學校應向學生和家長說明，妥善保管密碼和替代憑證 (例如 QR code) 的重要性。
- 如為學校配發的裝置 (例如平板電腦)，可使用裝置專屬 PIN 碼做為替代的安全驗證方式

套用合適的安全性設定

對全球各地的攻擊者而言，學校的裝置與網路都是有利可圖的明顯目標，因此請務必採用最完善的安全防護措施，以免造成服務中斷，損失資源、時間與金錢。系統管理員應根據機構使用的產品來啟用有效且合適的安全防護功能，同時確保教職員與學生可輕鬆使用相關系統。此外，系統管理員還須啟用重要的安全性和隱私權設定，避免使用者自行停用或修改這類設定，並採用其他具保護力的預設設定。請務必採用最完善的安全防護措施，以免造成服務中斷，損失資源、時間與金錢。如果學校使用 Chromebook，請參考本文末節建議的裝置政策設定。

最後，請將「資料最小化原則」納入安全性做法，以合理且適當的方式，有限度地收集、使用及揭露提供服務或進行相關業務所需的個人資訊。

應用程式和更新

請限制並盡量減少使用者可安裝的應用程式，因為安裝在裝置上的每個應用程式都可能是遭利用的攻擊媒介。盡可能使用出自可信任來源的應用程式。舉例來說，您可以請使用者檢查 Google Play 商店的驗證徽章，確認下載的官方應用程式已經過安全性審查。任何作業系統或硬體修改行為 (越獄解鎖或啟用 Root 權限) 都會造成重大安全漏洞，因此應一律避免。

存取權和瀏覽權限

管理員應確保使用者只能存取執行工作或學習所需的資料、軟體、服務和系統，防止非相關人員存取內容，並追蹤誰可存取哪些資源。請務必審查不同情境下可存取極機密資料 (例如使用者的個人識別資訊) 與系統 (例如人資、薪資、評分、安全性和設定) 的人員，並僅開放學校裝置與特定教職員存取這類資料來加強資安。

請檢查協作工具的資料共用政策，防止不當/過度共用及未經授權存取資料。限制或禁止校內人員 (尤其是學生) 對外分享資料，並落實敏感內容共用監控政策。

裝置遺失或遭竊

做好相關措施，就能在裝置遺失時保住資料。管理員應規劃一套標準程序，確保裝置遺失或遭竊後，人員仍能存取資訊和文件，例如在雲端環境中維護資料。請下載並列印兩步驟驗證程序的備用碼，避免帳戶存取權中斷。

如果獲報裝置遺失或遭竊，請盡可能從遠端鎖定裝置。這樣相關帳戶就會遭到鎖定或標記，防止他人未經授權存取學校資料。如果 Chromebook 遺失或遭竊，可從遠端清除其中內容。您還能監控 Google Workspace for Education 帳戶，查看是否有可疑活動，必要時甚至能將帳戶停權 (鎖定)。

對高風險使用者套用進階保護設定

Google 推出進階保護計畫，為經常曝光並擁有機密資訊的使用者 (包括 Google Workspace for Education 管理員) 提供額外保護。使用者可透過這項計畫防範針對性攻擊，例如網路釣魚陷阱、有害下載內容和密碼外洩。進階保護計畫專門協助 Google 帳戶抵禦針對性的線上攻擊，會自動採用高強度驗證和安全金鑰保護帳戶，並限制第三方存取帳戶資料。其他線上帳戶服務供應商也為高風險使用者提供高強度帳戶保護措施。如果學校 IT 管理員和教職員能存取個人資訊或技術系統，便應一律使用這些措施。

更新並升級系統

隨時更新裝置作業系統和應用程式，是所有人都能採取的重要自我保護措施之一。從幼兒園到高中的各級學校更應採取這項做法，因為在孩子的教育和日常生活中，學校是不可或缺的一環。教育和其他高風險環境面臨的惡意軟體攻擊，大多以 Windows 系統為目標，例如 SolarWinds、洛杉磯聯合學區勒索軟體攻擊、小石城學區網路入侵、Microsoft Exchange Server 資料侵害、阿布奎基學區勒索軟體攻擊，以及最近發生於聯邦機構的 Microsoft 軟體侵害行為。管理員可運用雲端產品和服務，更輕鬆地處理這方面的工作。這類產品和服務能減少攻擊途徑，並確保系統和應用程式隨時自動更新至最新版本。

升級至新式作業系統並定期更新

新版作業系統 (OS) 通常內含全新安全防護功能，更能防範已知攻擊途徑。因此，請務必啟用裝置 OS 中的自動更新功能。如果沒有這項功能，則至少每月從可信任的供應商網站下載並安裝更新和修補程式。

Chromebook 搭載 ChromeOS，不但經常自動更新安全性修補程式，確保系統快速採用最新安全性創新技術，還能在啟動前驗證唯讀作業系統的完整性。此外，Chromebook 還會將儲存在裝置上的所有資料加密，防止他人未經授權存取，並在獨立沙箱中執行每個網頁和應用程式。這樣一來，即使惡意軟體感染某個網站或應用程式，也不會散布到裝置的其他部分。

如果您的學校尚未計劃改用 Chromebook，但有升級現有裝置的需求，不妨考慮 ChromeOS 的 ChromeOS Flex 版本。ChromeOS Flex 提供一致的現代教學與學習體驗，並內建主動式安全防護和雲端式管理功能。有了 Flex，不必更換現有硬體，就能自動執行防護措施，並封鎖惡意執行檔和應用程式。

升級至新式瀏覽器並定期更新

請務必確保瀏覽器也會定期更新，且無安全問題。新式瀏覽器提供更先進的安全防護功能，使用者可依照瀏覽器提示輕鬆啟用，管理員也可在機構電腦上將這類功能調整為預設開啟，在網際網路上傳輸機密資訊時加以保護。請務必將瀏覽器更新至最新版本。不論是工作、學習或從事其他線上活動，使用最新版本的新式瀏覽器都能享有以下好處

- **採用強大的安全防護功能，**透過網站隔離和安全瀏覽功能，防止使用者意外前往危險網站
- **啟用自動更新功能，**確保瀏覽器快速取得安全性更新
- **確保連線安全無虞，**新式瀏覽器應使用傳輸層安全標準，使用者可在網址旁按一下，確認連線已標示為安全

Chrome 內建並預設開啟安全瀏覽等多項安全防護功能。此外，Chrome 的整合式密碼管理工具可在您瀏覽網站時自動填入密碼，讓您輕鬆使用高強度密碼。

使用即時快訊和監控系統

有了即時快訊和監控系統，學校就能快速識別威脅並做出回應，即時止損。請確保安全防護工具隨時在背景中運作，以持續收集並記錄整個系統的安全性事件。AI 工具特別適用於檢查系統收集到的大量資料，可從中找出異常狀況與模式，幫助您輕鬆快速地偵測威脅、處理及解決安全漏洞。IT 管理員或教職員可運用這類工具，安排系統活動的檢查順序。

學校可使用主要協作和通訊軟體 (例如 Google Workspace for Education) 內建的快訊和監控功能，也能另外部署安全性資訊和事件管理 (SIEM) 解決方案。

即時快訊和監控系統會追蹤整個學校的網路、裝置、應用程式、使用者和資料相關活動，例如使用者登入、檔案存取權、入侵跡象、資料竊取事件 (不論是否得手) 及管理員活動。

如果系統偵測到任何可疑活動，就會向學校的 IT 人員發送快訊，以便他們調查問題並採取行動來降低威脅。

此外，學校可使用快訊和監控工具構成的即時系統，深入分析威脅相關資料，找出攻擊趨勢和模式，更有效地確保資安。

下列是快訊和監控 (含 SIEM) 系統的最佳使用方法：

1. **制定安全性目標**
   学校にとって最も重要な情報とシステムはどれか、どのような辨別哪些是學校不可或缺的資訊與系統，並瞭解這些資訊及系統最可能遭遇哪些類型的威脅。接著請根據這些威脅判斷您需要收集哪些資料來監控情況。
2. **收集合適的資料並妥善設定應用程式**
   為達成最迫切的安全性目標，請務必收集合適的資料並設定應用程式。這裡所指的資料可能來自防火牆、內容篩選器、入侵偵測系統、網路伺服器，其他安全性裝置、通訊和協作軟體、學校資訊系統，以及學習管理系統。
3. **調查快訊指出的問題並做出回應**
   監控系統發布快訊時，務必調查快訊指出的問題，並採取適當行動。例如集結多個團隊共同調查快訊來源、判斷快訊是否為誤判，或採取行動防範威脅，包括將帳戶停權、重設使用者密碼、隔離或刪除電子郵件、變更檔案權限，或移除裝置。

向教職員和學生提供資安訓練

從幼兒園到高中的各級學校均應提升學校社群的安全意識和習慣，並透過活動與合作夥伴關係，協助使用者培養相關能力。請務必向教職員和學生說明資訊安全的重要性，以防範重大網路安全威脅，並幫助他們在網路世界中保護自己。請教導他們如何使用機構既有的產品和服務，找出及回報網路釣魚電子郵件等威脅；最重要的是，他們必須瞭解如何採取行動預防這些攻擊。學校和學區應提升學校社群的安全意識和習慣，並透過活動與合作夥伴關係，協助使用者培養相關能力。

如何安全使用裝置和軟體

管理員可以與老師和專家合作，設計適合不同年齡的網路安全課程，幫助學生瞭解如何安全地使用裝置、軟體及系統。學校或學區可以根據情況，製作專屬訓練教材為師生提供建議，也能直接使用現成教材 (例如 Google 安全中心的 Be Internet Awesome 和 Khan Academy)，然後依需求調整。無論是學校或社群使用者，這些計畫都能協助保護他們的安全。

辨別威脅

透過訓練教導學生和教職員如何辨別威脅，也是保護他們安全的重要做法。孩子可能不知道如何判斷某個內容或行為是否合理，因此必須學習分辨幾種不同的威脅，並瞭解回報方式。對此，管理員應將訓練重點放在投資報酬率最高的幾個主題，而且除了說明辨別威脅的方式外，也應加強宣導因應措施。使用者需能分辨的常見威脅包括勒索軟體、網路釣魚、社交工程、惡意軟體和詐騙。如果機構更常遭遇特定威脅，請務必確保學校社群瞭解相關知識。

安全共用資料和檔案

機構應提供訓練，幫助教職員瞭解如何以適當方式共用檔案和資料，以及辨別透過電子郵件發出的不當要求。最重要的是，教職員應只在必要時共用或處理個人機密資訊，並採取額外保護措施來保障資料安全，例如絕不透過電子郵件共用或對外分享。管理員應使用資料遺失防護功能 (ChromeOS 和 Workspace for Education 皆有該功能)，警告或防止使用者共用含身分證字號等機密資料的檔案，或將敏感內容複製並貼到網域外部。

Google 採取的安全性做法：教育裝置和服務

採購軟體是學區可採取的最佳保護措施之一。軟體應採用穩固可靠的架構和設計，盡可能減少安全漏洞出現的風險，並在各層內建安全防護機制。透過要求學校購買安全軟體，或向安全追蹤記錄經驗證的公司購買軟體，可有效避免更多種網路風險。例如，Google 強化了 ChromeOS，同時繼續部署更主動且更智慧的解決方案，並善用我們的強項，將機器學習、雲端和身分識別的專業知識應用其中。

Google 致力打造可保護師生隱私權的產品，同時為機構提供業界最佳的安全性。Google for Education 的產品與服務能持續防範日益複雜的威脅來保護使用者、裝置和資料，值得您的信賴。學校 IT 管理員可透過本節瞭解使用 Google for Education 產品時的安全性建議。

Google Workspace for Education

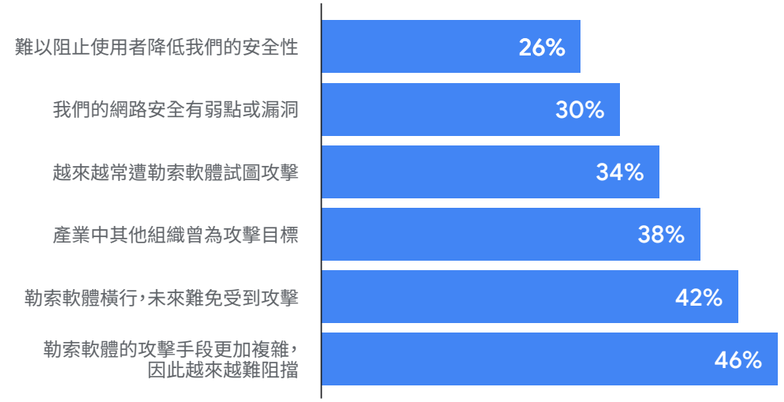
Google Workspace for Education 是一套專為學校提供的 Google 工具和服務，方便使用者協作、簡化教學程序，並提供安全的學習環境。Google for Education 的產品與服務能持續防範日益複雜的威脅來保護使用者、裝置和資料，並提供多項安全性工具，包括快訊和安全中心、電子蒐證專用保管箱、身分與存取權管理，以及資料遺失防護功能。

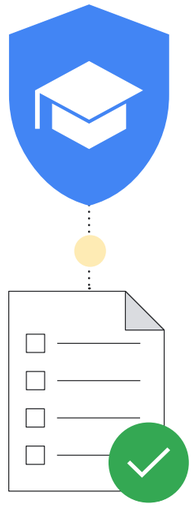
如果您剛開始使用 Google Workspace for Education，可以參閱我們整理的實用教材，根據本指南的建議進行設定。若要瞭解如何開始使用 Google Workspace for Education，請參閱這份快速入門 IT 設定指南。

安全性檢查清單

請參閱安全性檢查清單，進一步瞭解如何強化機構的安全性和隱私權。如果學校採用 Google Workspace for Education Standard 或 Google Workspace for Education Plus，還可以透過「安全性狀態」頁面監控管理控制台的設定。舉例來說，您可以查看電子郵件自動轉寄、裝置加密、雲端硬碟共用等設定的狀態。如有需要，您也可以根據一般安全性指南與最佳做法調整網域設定，並全盤考量機構的業務需求和風險管理政策來採行指南中的建議。

教育機構預期遭受攻擊的原因





資料來源: https://assets.sophos.com/X24WTUEQ/at/g523b3nmgcfk5r5hc5sns6q/sophos-state-of-ransomware-in-education-2021-wp.pdf

此外，您可以參考下列其他實用訣竅，充分發揮 Google Workspace for Education 內建防護功能的效用：

設定機構單位

各 Google Workspace for Education 帳戶可能適合不同的設定。設定機構單位後，就能將使用者歸類到不同群組，然後提供相應的服務、設定和權限。例如，對教職員採用兩步驟驗證，以及對低年級學生採用適齡的驗證方法。因此，請為教職員和學生分別設定機構單位，並對各組使用者套用政策。如要有效及靈活地管理 Google Workspace for Education 帳戶，就必須具備設計完善的架構。

設定密碼政策和管理員帳戶保護措施

如先前所述，使用者驗證是保護機構安全的一大重點。因此我們設定數種彈性的驗證管理方式，讓管理員確保使用者帳戶獲得適當的安全防護。設定密碼政策，強制使用者建立高強度密碼。在適當情況下，可根據「安全登入」部分的建議分組方式，要求使用兩步驟驗證。您可以對部分使用者強制執行兩步驟驗證 (記得給他們時間設定)，並使用多種方式部署這項機制，包括安全金鑰 (最安全)、Google 提示 (使用 Android 和 iOS 裝置上的 Google 應用程式)、驗證碼產生應用程式 (例如 Google Authenticator)，以及簡訊或電話 (這兩種是最不安全的方式)。

如果機構採用 Google 以外的第三方識別資訊提供者服務，可以透過該服務設定單一登入。您還可以根據需求，對超級管理員以外的帳戶同時套用兩步驟驗證與單一登入。

開啟或關閉服務

管理員可在 Google 管理控制台中，控管使用者能透過他們的 Google Workspace for Education 帳戶存取哪些 Google 服務。只要依機構單位開啟或關閉服務，即可控管 Google 日曆、雲端硬碟、Meet 等 Google 服務的存取權 (您也可以使用群組開啟服務)。啟用 YouTube、Google 地圖和 Blogger 等額外服務前，也可以先瞭解 Workspace 核心服務和額外服務的差異。建議管理員依年齡設定 Google 服務存取權。另請注意，未滿 18 歲的使用者登入 Google Workspace for Education 帳戶後，系統將在部分服務中自動套用限制。

此外，您還能使用情境感知存取權 (Workspace for Education Standard 和 Workspace for Education Plus)，根據裝置的 IP 位址、地理位置來源、安全性政策或 OS，允許或禁止使用者存取 Gmail、雲端硬碟和日曆等 Google 應用程式。舉例來說，您可以僅允許在特定國家/地區，透過公司擁有的裝置使用雲端硬碟電腦版。

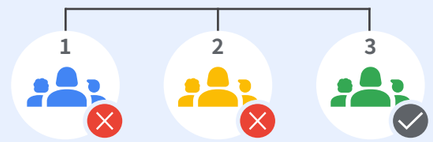
授權使用者存取服務的方法

在 Google 管理控制台中，可關閉機構單位的 Google 服務存取權，例如 Google 雲端硬碟。

如果該機構單位的部分使用者需要使用雲端硬碟，以下 2 種做法可供選用：

1. 將使用者移至已啟用雲端硬碟的機構單位。
2. 將使用者加入存取權群組，並為該群組啟用雲端硬碟。這樣一來，即使群組成員所屬機構單位關閉雲端硬碟服務，他們依然能夠存取。

機構單位



機構單位 1 和 2 已關閉 Google 雲端硬碟

存取權群組內

但是機構單位 1 和 2 的**存取權群組**使用者仍可存取 Google 雲端硬碟

資料來源: https://support.google.com/a/answer/9050643?sjid=4805599982673626852-NA

設定資料共用政策和保留規則

管理員可控管使用者能否與機構外部人員共用 Google 雲端硬碟檔案和資料夾，避免意外/過度共用資料和檔案，防止資料外洩。請務必分隔檔案和磁碟機、建立機構單位，並根據最低權限原則執行作業，以便在攻擊者入侵帳戶時，阻擋他們繼續跨網路移動。潛在攻擊者能存取的資料和網路越少，損害就越小。

請為學生停用外部檔案共用功能 (或只允許與許可的外部網域共用檔案)，並將「存取權檢查工具」設為「僅限收件者」。如果您允許部分或所有使用者將檔案分享到網域外部，請開啟警告。這樣一來，當使用者這麼做時，系統就會顯示警告訊息。此外，請停用在網路上發布檔案的功能，並要求外部協作者使用 Google 帳戶登入。

Workspace for Education Standard 和 Workspace for Education Plus 的客戶還可以定義目標對象及建立信任規則，詳細設定共用建議和限制。舉例來說，您可以設定目標對象，將老師的預設連結共用對象改為「教職員」，而不是機構內所有人。您也能建立信任規則，禁止低年級學生將檔案分享給高年級學生。

請檢查共用雲端硬碟政策，確保只有適當使用者能建立共用雲端硬碟，並防止外部使用者存取這些雲端硬碟。建議您只允許管理員 (或教職員) 建立共用雲端硬碟，然後由您直接管理相關存取權。

請盡可能限制目錄瀏覽權限和聯絡人共用功能。您可以停用部分或所有使用者的聯絡人共用功能，也能建立自訂目錄，決定誰可查看哪些使用者的個人資料。

在雲端硬碟和 Gmail 中設定資料遺失防護政策，即可偵測及封鎖機密資訊。您可以運用預先建立的政策，保護銀行帳號、信用卡號碼等一般機密資訊，也能根據關鍵字、字詞清單和規則運算式自訂政策。

管理 Gmail 設定

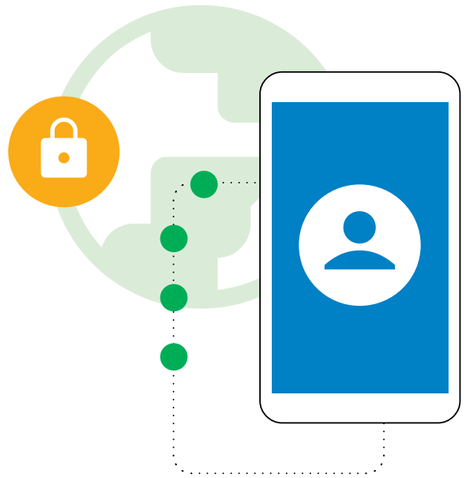
Gmail 是 Google Workspace for Education 的一項核心服務，管理員可運用其中許多設定，保護機構和使用者安全。您可以使用 Gmail 驗證來防範垃圾郵件、假冒郵件和網路釣魚郵件。您也能自訂垃圾郵件篩選器設定，包括要求所有經核准的寄件者進行寄件者驗證，以及對內部寄件者停用垃圾郵件篩選器略過功能。

請盡可能停用 POP/IMAP 存取權，並啟用加強型送達前掃描郵件功能，以及網路詐騙和惡意軟體進階防護措施。如果您允許部分或所有使用者收發外部電子郵件，可以啟用外部收件者警告功能。

Google Workspace for Education Standard 和 Google Workspace for Education Plus 的客戶還可使用安全沙箱設定規則來偵測有害附件，防範電子郵件夾藏的惡意軟體和勒索軟體。

第三方應用程式

請使用內建核准工作流程，核准哪些第三方應用程式可透過 API 存取帳戶資料，進一步防止未獲授權的非校用應用程式共用資料。



報告與監控

管理員可以透過 Google 管理控制台查看報告和記錄事件，掌握機構的活動 (例如潛在安全性風險)、得知登入者的身分和登入時間，並瞭解使用者建立及共用內容的方式。除了網域層級資料外，管理員還能檢閱精細的使用者層級詳細資料圖表。查看報告和稽核記錄 (包括快訊中心)，即可找出安全性風險、分析服務使用情形、診斷設定問題及追蹤使用者活動等等。

Google Workspace for Education Standard 和 Google Workspace for Education Plus 的管理員皆可在安全性資訊主頁中，查看各種安全性報告總覽、判斷趨勢，還能比較目前和歷來資料，例如雲端硬碟的檔案共用情形、Gmail 的垃圾郵件、網路釣魚攻擊和惡意軟體活動，以及可疑的使用者帳戶登入行為與裝置活動。系統會提供六個月內的大多數使用情形、活動、稽核記錄 (包括管理員、雲端硬碟、Meet 和 Chat 記錄事件) 與安全性報告。

運用安全中心

Google Workspace for Education Plus 和 Google Workspace for Education Standard 的管理員皆可透過安全中心查看進階安全性資訊和數據分析，進一步掌控安全性問題影響網域的情形。

安全中心提供安全調查工具，可協助管理員找出網路釣魚攻擊、不當的檔案分享情形、可疑的使用者和裝置活動等安全性和隱私權問題，然後加以分類並採取適當措施。

Google Workspace 是世界上最安全的雲端原生通訊與協作套件

0

自 2021 年 11 月以來，Workspace 中遭利用的安全漏洞數量為 0*

50%

使用 Workspace 預計可省下 50% 的網路安全保費

少2倍

與 Microsoft 365 相比，使用 Workspace 的機構遭遇的安全性事件數量少 2 倍

少2.5倍

與 Microsoft Exchange 相比，使用 Workspace 的機構遭遇的安全性事件數量少 2.5 倍

*根據 CISA，這個數字大幅低於相同領域的其他效率提升產品/服務供應商。

Google Chromebooks for Education

Chromebook 電腦內建立即可用的安全防護功能，能有效抵擋威脅、可擴充且容易上手，非常符合師生需求。無論企業、學校或消費者使用的 ChromeOS 裝置，都未曾回報遭遇勒索軟體攻擊。Chromebook 運用最新功能協助學校防禦日新月異的威脅，且會自動在背景中更新，因此使用者很快就能繼續處理工作。

自動更新作業系統和應用程式，並內建惡意軟體防護機制

攻擊者會不斷利用作業系統、瀏覽器和熱門應用程式中的錯誤和漏洞，企圖安裝惡意軟體並竊取使用者資料。Chromebook 內建強大防護機制，且會執行安全性更新，可確保 OS 與應用程式均隨時更新，保護您和您的使用者。這款電腦採用雲端應用程式，不必像本機應用程式一樣進行軟體更新。此外，Chromebook 搭載 Google 設計的安全晶片，能保護裝置和使用者身分識別資訊，並確保系統完整性。

校內機群中的 Chromebook 會自動將惡意軟體防護機制更新至最新版本。裝置內建資料加密、驗證開機程序、沙箱機制、自動更新等安全防護功能，可協助師生防範網路威脅

保護使用者資料

使用 Google 帳戶登入 Chromebook 後，所有資料都會儲存在加密檔案中，因此裝置上的使用者無法查看他人資料，或透過他人帳戶登入應用程式。這樣一來，學生就能輕鬆安全地共用教室內的裝置，學校也可降低運算總成本。如想取得更多進階安全防護功能，可購買 Chrome Education 升級版裝置管理授權，進一步掌控安全性狀態。

針對使用者自行管理的裝置，從遠端控管安全性政策

學校管理員可透過 Google 管理控制台，從遠端設定 ChromeOS 政策並安裝/更新應用程式。IT 管理員只需按下按鈕，就能立即更新數十萬部 Chromebook 的政策和設定

這能確保：

- 學生僅能存取學校核可的內容和應用程式
- 所有應用程式和擴充功能會自動安裝最新安全性修正
- 使用者無法將裝置中的學校資料複製、轉移或分享到外部
- 根據資料和 Google 提供的專屬建議做出決策，有效解決安全性威脅
- 直接在管理控制台中，集中控管所有使用者的安全性、身分與存取權管理政策

管理員應設定以下重要政策：

裝置政策

- **訪客模式**
  我們建議停用裝置的訪客模式，讓師生必須以自己的憑證登入，而無法匿名使用裝置。
- **登入限制**
  請勿讓師生使用個人 Gmail 帳戶登入學校的 Chromebook。您可以強制執行登入限制，僅限學生專用裝置登入 Workspace 網域。
- **使用者和裝置回報功能**
  建議管理員開啟使用者和裝置回報功能，以便收集所需指標，例如 Chromebook 的使用頻率、使用者身分和硬體狀況。
- **強制重新註冊**
  管理員如未取消佈建，學校擁有的 Chromebook 就必須留在校內。建議管理員啟用 Chromebook 的強制重新註冊功能。這樣一來，只要 Chromebook 遭抹除或失竊，就會自行重新註冊。

使用者政策

- **無痕模式**
  學校的 Chromebook 應提供學生良好的學習體驗，包括僅讓學生使用經驗證的瀏覽器、透過網路內容篩選器防止他們接觸不當網站。管理員應停用無痕模式，讓學生無法規避網路內容篩選器。
- **Proxy 模式**
  如果學校使用 Proxy 篩選網路內容，請務必禁止使用者自行變更 Proxy 設定。
- **多帳戶登入存取權**
  如果使用者能同時使用 Workspace 帳戶和另一個帳戶登入學校的 Chromebook，很容易將學生或學校的機密資料/資訊竊取至另一個帳戶。因此，建議管理員禁止多帳戶登入存取權
- **瀏覽器記錄**
  我們建議為學生停用清除瀏覽器記錄的功能。萬一發生網際網路安全事件，相關歷史記錄可能會在調查期間派上用場。

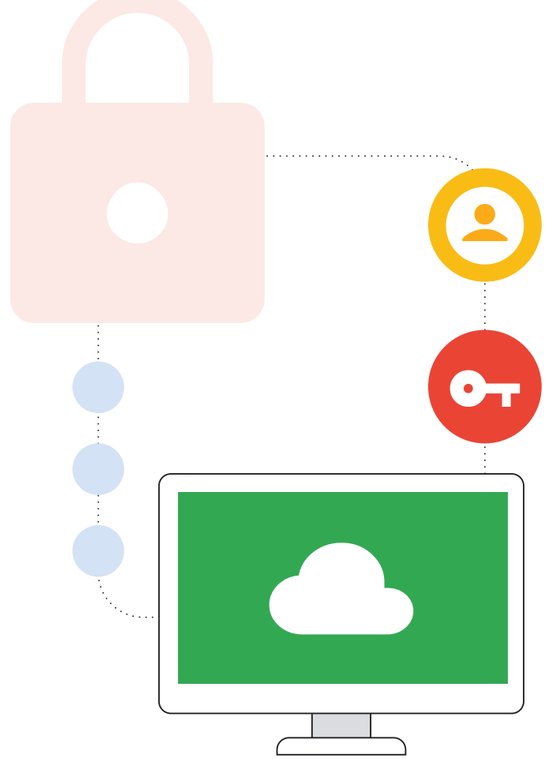
如要防止常見錯誤造成重大網路事件，可以採用以上政策。如要瞭解其他建議的安全性政策，請參閱這份安全性檢查清單。

遠端管理政策，隨時隨地安全使用端點裝置

有了 ChromeOS 的遠端政策管理系統，學校管理員不必透過學校的網路伺服器，就能直接在裝置上套用安全性設定，並執行內容篩選系統等安全性工具。因此，不論在家中或教室，學生使用學校的 Chromebook 時，都能享有一致的安全防護。由於學校紛紛採用數位教科書與線上學習工具，而學生也需要將電腦帶回家中完成作業，遠端管理政策的做法日趨重要。

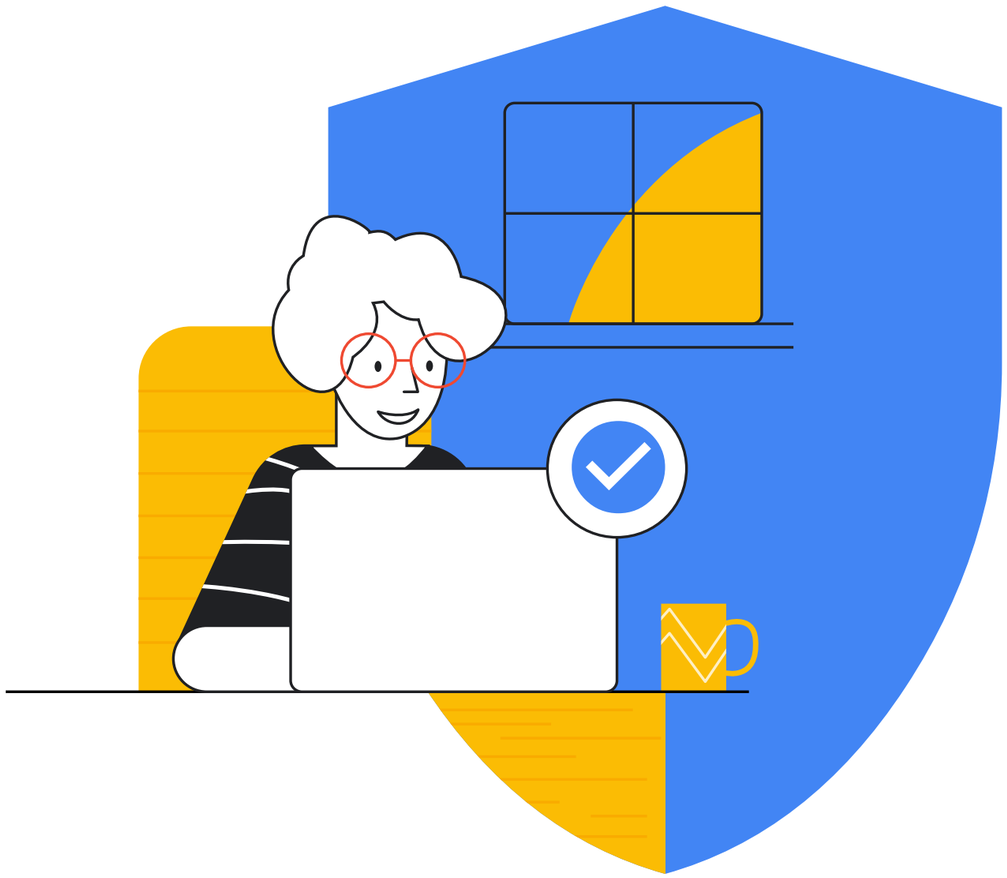
結語

保護從幼兒園到高中的各級學校不受網路事件影響，是牽涉許多層面的複雜挑戰，但為了保護您自己、學生、教職員和更廣大的線上生態系統，仍建議在這方面多下心力。您可以從本文提及的要點著手準備，不過每間學校仍需配合自身需求調整這些建議做法，並持續瞭解新興技術及不斷變化的威脅情勢。籌備從幼兒園到高中的各級學校 安全計畫時，不妨使用這份指南來奠定基礎，瞭解有哪些可行的後續步驟與措施。此外，Google 還有各種資源、訓練課程和眾多出色的網路安全專家，可幫助學校和機構按照這份指南加強安全防護，並採用 AI 等新興技術。Google 的教學專用產品為學校提供多項現成解決方案，防範 前述的網路安全陷阱。我們很樂意為您提供協助，攜手共同 制定並實推行您的安全性計畫。



資源清單

- Google，《協助你確保線上安全的工具和提示》，Google 安全中心，https://safety.google/intl/zh-tw/security/security-tips/，檢索日期：2022 年 10 月 6 日。
- NIST，《Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1》(關鍵基礎建設的網路安全改善架構 1.1 版)，NIST Technical Series Publications (NIST 技術系列刊物)，2018 年 4 月 16 日，https://doi.org/10.6028/NIST.CSWP.04162018，檢索日期：2022 年 10 月 6 日。
- Microsoft，「Microsoft AccountGuard Program」(Microsoft AccountGuard 計畫)，Microsoft AccountGuard Program，https://www.microsoftaccountguard.com/en-us/，檢索日期：2022 年 10 月 6 日。
- Google，「進階保護計畫」，Google 進階保護計畫，https://landing.google.com/intl/zh-tw/advancedprotection/，檢索日期：2022 年 10 月 6 日。
- Google，「Google 安全中心」，Google 安全中心：確保線上安全，https://safety.google/intl/zh-tw/，檢索日期：2022 年 10 月 6 日。
- Meta，《基本入門：保護帳號安全》，保護帳號安全，https://zh-tw.facebook.com/gpa/resources/basics/security，檢索日期：2022 年 10 月 6 日。
- Meta，《Facebook Protect》，Facebook，https://www.facebook.com/gpa/facebook-protect，檢索日期：2022 年 10 月 6 日。
- NIST，《SP 800-124 Rev. 1: Guidelines for Managing the Security of Mobile Devices in the Enterprise》(SP 800-124 修訂版 1：企業行動裝置的安全管理指南)，NIST Technical Series Publications (NIST 技術系列刊物)，https://doi.org/10.6028/NIST.SP.800-124r1，檢索日期：2022 年 10 月 6 日。
- 密碼金鑰：https://developers.google.com/identity/passkeys
- CISA《Protecting Our Future Cybersecurity K-12 Report》(保護我們的未來：幼兒園到高中各級學校網路安全報告) https://www.cisa.gov/protecting-our-future-cybersecurity-k-12
- GAO 報告 https://www.gao.gov/products/gao-20-644
- 如要進一步瞭解 Google for Education 能如何協助您保護貴機構，請前往 Google for Education 隱私權與安全中心。
- Zcaler 網路釣魚報告



Google for Education