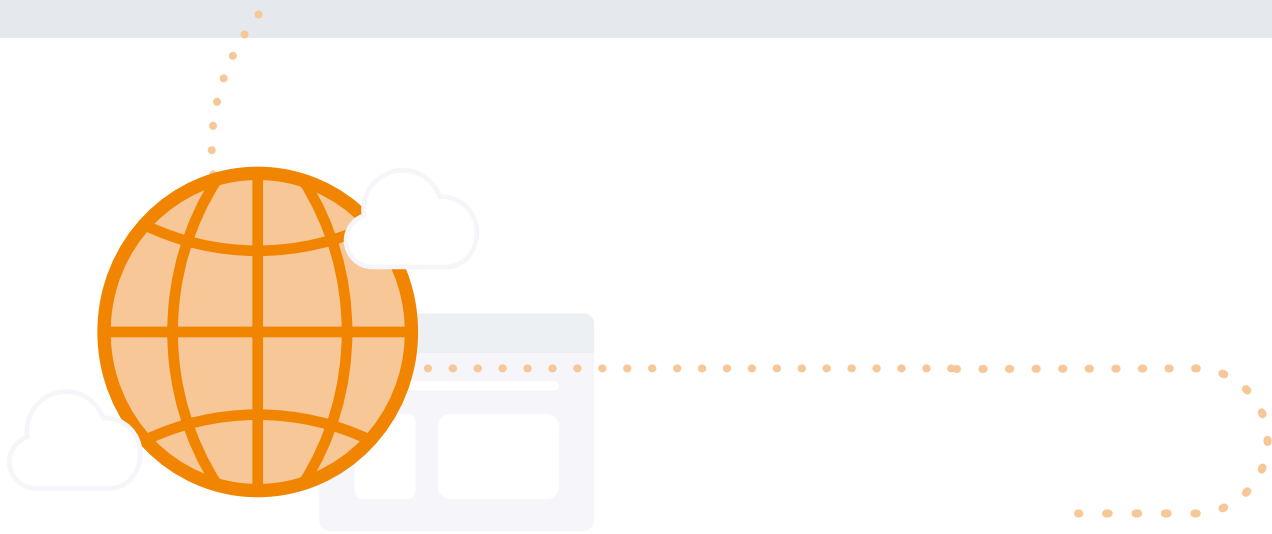




# K-12 學校網路 內容過濾基礎指南



全球各地的學校都在試著找到網際網路平衡點：他們既希望讓學生能夠利用網路上豐富的研究與學習資源，同時也希望能夠保護他們的安全，讓他們遠離危險或不當的內容，還有釣魚者和有心人士等。

孩子們每天都試圖在學校存取不當或危險的內容：在紐西蘭，學校最近的報告指出，他們在一個月內封鎖了 3.99 億次存取不當內容的嘗試。<sup>1</sup>

現在，學生會把學校配發的裝置帶回家，在學校防火牆之外的環境使用裝置。因此，學校需要一套機制，無論學生身在何處，都能有效阻擋裝置存取不適當的網站。

這也就代表著學校必須從多個方面解決學生安全問題。本指南的目的就是幫助學校順利應對這項挑戰。



## 本指南將討論以下內容：

- 哪些線上內容可能會使學生面臨風險，以及我們為何應該更積極地保護他們
- 有哪些細微差異和特殊情況需要採用彈性且客製化的內容過濾方式
- 如何教育並賦能學生理解數位公民身份
- 以及 Jamf 可以如何幫助您



# 為何需要過濾？

原因可多了。





## 保護學生

各國對於學生的網路存取權限有不同的法律規範，但整體來說，都涵蓋以下幾個重點：

- 色情或猥褻內容
- 仇恨言論、暴力或激進網站
- 鼓勵自殘、自殺或厭食症的網站
- 網路釣魚與網路威脅者
- 網路霸凌
- 移除社群媒體與遊戲等干擾因素
- 賭博網站

根據世界衛生組織的資料，15-19 歲的青少年是全球自殺的第四大死因群體。<sup>2</sup> 而在學齡學生中，大約有 47-60% 的學生遭遇過網路霸凌，這些數據顯示，<sup>3</sup>保護學生免受這類網路危險，確實可能拯救生命。

## 學生專注力與學習成效

限制學校環境中的社群媒體不僅能減少網路霸凌的機會，還能幫助學生更專注於課業。這能夠提升學生的學習效率與課堂參與度。

### 例如

美國國會於 2000 年通過了《兒童網路保護法》（CIPA），將學校的網路安全政策與 E-rate 計畫的折扣綁定在一起。

在英國與威爾斯，教育部於 2015 年發布了《保護兒童教育安全》指導原則，要求學校確保有適當的過濾和監控系統。蘇格蘭也有類似的規定<sup>4</sup>

世界各地（除了南極洲）都有類似的法規或要求。

## 系統安全

具備過濾惡意軟體（malware）、廣告軟體（adware）及間諜軟體（spyware）的過濾機制，可確保學生的上網安全。同時，這也能維護學校的網路安全。

## 監控與報告

家長需要確保孩子不會接觸到不適當的內容，而學校則有責任監控網路使用狀況，以保障數據安全與學生安全。

不過，這一切必須兼顧學生的隱私權，避免對個別裝置過度的檢查與干涉。整體規劃應該是一個透明的過程，透過匿名化資料的收集，並將結果呈現給資安專家、家長與學校管理者。

學校應選擇能提供端點保護與網路威脅防禦的安全工具，例如 [Jamf Protect](#) 和 [Jamf Safe Internet](#)。這些工具應具備以下功能：防範已知的病毒，透過行為分析發掘並隔離新的潛在威脅，以及完整的報告系統此外，學校應選擇具有強大社群支持的解決方案，例如 [Jamf Nation](#) 或 [Jamf Educator](#)，這樣使用者可以交流最佳實踐，並獲得其他教育工作者的建議。若搭配 [Jamf School](#) 或 [Jamf Pro](#) 這類完整的行動裝置管理（MDM）解決方案，將能更全面地管理學校的裝置與網路安全。



## 為什麼不乾脆全部封鎖？

既然資料顯示出學生是十分容易受到網路傷害的，有的家長或教育者可能會認為那何不封鎖所有資訊就好？但這可能在多方面造成問題。

首先，不管是教室還是學生，一定都會需要使用網路上的資源，有的學校可能會因為過於激進地保護學生封鎖所有網站例如，YouTube 或 Google 對許多課堂教學是十分重要的。如果教師想要教育學生關於時事、社會運動和其他主題，卻發現自己無法存取這些教育內容，而且也不能透過網路輕鬆地收作業，可能會感到相當困擾。

然而，完全不加限制地開放這些服務也可能帶來問題。也就是為什麼您需要像 [Jamf Safe Internet](#) 這樣的解決方案，能夠針對網站內容進行更精細的過濾，而不僅是依照域名過濾，這樣才能同時保護學生並提供有效的學習支持。

沒有任何過濾系統是完美的。總有人需要持續追蹤惡意軟體與釣魚網站，並將其加入封鎖清單，而新的惡意網站也不斷被創建。

因此，教育的一部分應該是幫助學生學會在沒有限制的環境中安全上網，畢竟這就是他們在未來必須面對的網路環境。已經具備網路風險意識並知道如何保護自己的年輕人，將比完全被動受限於過濾系統的學生更了解網路安全。



## 學生作為數位公民

學生教育的一部分應該包括如何避免網路釣魚、惡意程式、誤導性資訊等，即使學生離開學校及其內容過濾系統之後，仍能保有這些技能。

教育和培訓學生成為聰明的數位公民應該被納入課程設計與教學方針中。這包括如何透過批判性思維技能來理解何為可靠的來源，學習哪些來源值得信賴，如何避免釣魚攻擊和其他詐騙。

如果老師希望幫助學生更輕易地掌握他們的數位生活，建議從 Common Sense Education 的數位公民計畫開始，這裡有免費的、現成可教的課程、教材和教學建議。Common Sense 是一個總部位於美國的非營利組織，致力於改善所有兒童和家庭的生活，並與哈佛大學教育研究所的 Project Zero 合作開發這些課程。課程內容依照年級/年齡分組

# 如何選擇適合的過濾和安全解決方案？

如何判斷哪個解決方案最適合貴校？一開始時，您可以問潛在供應商以下六個問題：

## 1 是否能過濾所有裝置，包括 iPad 和 Mac？BYOD（自備裝置）呢？

解決方案需要在學校中提供全面性的覆蓋過濾系統的效能與優劣取決於其最薄弱的環節。

## 2 如何防範未知的攻擊者？

確保所使用的系統能夠整合行為分析和即時警報，來捕捉未知網站或惡意程式，如同 [Jamf Protect](#) 的功能。行為分析可以通過了解惡意程式和危險網站的行為模式或常用詞語，及時制止其惡意行為。

## 3 它能對像 YouTube 或 Google 這樣的網站進行部分封鎖嗎？

YouTube 和 Google 雖然已成為強大的學習工具，但它們同時也可能讓學生接觸到未經過濾的內容。因此，學校需要一套工具，確保 Google 安全搜尋（Safe Search）和 YouTube 限制模式（Restricted Mode）開啟，且無法被使用者關閉。

## 4 此解決方案如何讓父母參與其中？

有些家長可能會質疑過濾的必要性，也有些家長可能會對過濾功能是否過於嚴謹或寬鬆而有所顧慮。讓家長能夠透過像 [Jamf Parent](#) 這樣的應用程式，查看孩子的網路活動，並提供像 Jamf 一樣清楚且詳盡的安全和隱私報告，將有助於緩解這些顧慮。

## 5 如何過濾學生在校外使用的裝置？

不管是哪一種解決方案，都必須確保它能過濾和管理家中及學校的學生裝置：就像 [Jamf School](#) 一樣。如果家長能夠透過像 [Jamf Parent](#) 這樣的易用應用程式來增強過濾和管理功能，那就更好了。

## 6 如何與我的其他解決方案整合？

一個能夠與 MDM（行動裝置管理）供應商無縫合作的過濾和安全解決方案，並能與可信的供應商合作，不僅提供世界級的安全性，還能增加更多教育選項，為您帶來更多價值。

# 有什麼 Jamf 幫得上忙的地方？

Jamf 提供完善的 Apple 管理與安全解決方案除了行動裝置管理（MDM），Jamf 還提供從學校管理層到家長端的支援工具，同時幫助學生發揮最大學習潛能。



## jamf | SCHOOL

讓 IT 與教育工作者有效率地管理 Apple 裝置

## jamf | PROTECT

專為 Mac 設計的端點防護



## Jamf Safe Internet

針對教育領域開發的內容過濾與威脅防禦



Jamf  
Teacher



Jamf School  
Student



Jamf  
Parent



Jamf  
Assessment

## jamf | EDUCATOR

提供客戶教育資源，幫助學校充分利用 Jamf Teacher 應用程式。

## jamf | MARKETPLACE

各種與 Jamf 平台整合的附加功能。

Jamf Safe Internet 是學校確保學生安全上網的關鍵工具，並能同時保護學生隱私：

- 支援 macOS、iOS 及 ChromeOS，確保裝置安全，不受環境限制
- Jamf Protect 透過行為分析監控裝置，防範未知攻擊
- Jamf Safe Internet 強制啟用 Google 安全搜尋與 YouTube 限制模式，防止使用者自行關閉
- Jamf Safe Internet 以裝置為基礎，可在學校網路之外運作，而 Jamf Parent 也為家長提供額外工具，協助保護校外裝置的安全
- 尊重隱私：Jamf 除了遵守所有適用的隱私法規外，還簽署了 [學生隱私保護承諾 \(Student Privacy Pledge\)](#)，展現我們對學生、家長與教師資料保護的承諾。



Jamf Safe Internet 無縫整合至 Jamf Teacher、Jamf School Student 及 Jamf Parent 應用程式，能夠大幅提升學校現有的工作流程效率。

[立即試用](#)

或聯繫您的授權經銷商以獲取更多資訊！