

Google for Education

運用 Google Workspace for Education 付費版本的 30 多種方法

goo.gle/use-edu-workspace



簡報使用方式

本簡報精選出幾種 Google Workspace for Education 付費版的熱門用途。這些工具能提升資料安全性、教學成效、學生參與度和全校性協同合作，還有許多其他功能。

這份簡報會依序介紹產品功能、常見用途，以及簡易的功能使用操作說明。請查看整份簡報，瞭解 Google Workspace for Education 可提供您多少功能。

Google Workspace for Education 付費版

Google Workspace for Education 的三種付費版本能為貴機構提供更多選擇、掌控權和使用彈性。



Google Workspace for Education Standard

進階安全性與分析工具讓你能進一步瞭解與掌控整個學習環境，進而降低風險及削弱威脅。



Teaching and Learning Upgrade

進階教育工作者工具能讓溝通互動與課程體驗變得更加豐富多元，並引導學生建立學術誠信。



Google Workspace for Education Plus

這套全方位的解決方案除了包含 Education Standard 和 Teaching and Learning Upgrade 的所有功能，還額外提供更多選項，能為學校社群提供成效最佳的整合式學習環境。

目錄



安全性與分析工具

Education Standard 和 Education Plus 的各項工具

調查工具

- 分享不當內容
- 不小心共用檔案
- 電子郵件分類
- 網路詐騙和惡意軟體電子郵件
- 阻止不肖人士

安全性資訊主頁

- 大量垃圾郵件
- 對外共用檔案
- 第三方應用程式
- 網路詐騙

安全性狀態

- 針對風險區域的建議做法
- 即時掌握最佳做法
- 安全性最佳做法
- 為人數漸增的學校提升安全性

進階管理控制項

- 資料相關法規
- 授權相關法規
- 應用程式限制
- 管理行動裝置
- 遷移資料

目錄



教學與學習工具

Teaching and Learning Upgrade 和 Education Plus 的各項工具

原創性報告

- 偵測抄襲內容
- 將抄襲偵測功能變成學習機會

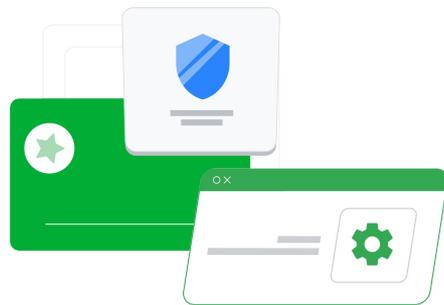
Google Meet

- 安全的視訊會議
- 提高視訊會議安全性
- 錄製課程
- 錄製教職員會議
- 錯過的課程
- 直播會議
- 直播學校活動
- 提出問題
- 收集意見
- 學生小組
- 追蹤出席狀況



安全性與 分析工具

透過主動式安全性工具抵禦威脅、分析安全性事件，並保護學生與教職員資料，進一步控管貴機構網域。



[調查工具](#)



[安全性資訊主頁](#)



[安全性狀態頁面](#)



[進階管理控制項](#)



調查工具

這是什麼？

使用調查工具找出網域內的安全性和隱私權問題，然後加以分類並採取適當措施。

用途

分享不當內容



[逐步操作說明](#)

不小心共用檔案



[逐步操作說明](#)

電子郵件分類



[逐步操作說明](#)

網路詐騙/惡意軟體電子郵件

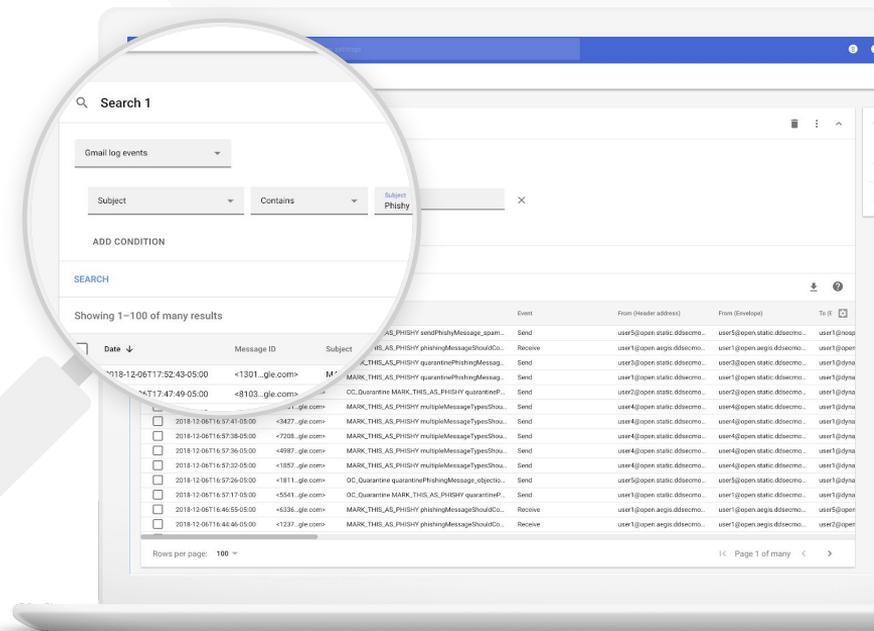


[逐步操作說明](#)

阻止不肖人士



[逐步操作說明](#)



“

我得知有人分享含有不當內容的檔案。
我想知道是誰建立了這個檔案、建立的
時間、共用者與共用的對象，以及誰編輯
過檔案，而我想刪除這份檔案。”

[逐步操作說明](#)

分享不當內容

調查工具中的雲端硬碟記錄可用來尋找、追蹤、隔離或刪除貴機構網域中的不當檔案。存取[雲端硬碟記錄](#)可讓您：

- ✓ 根據名稱、執行者和擁有着等條件搜尋文件
- ✓ 查看該文件的所有記錄資訊
 - 建立日期
 - 文件擁有着、檢視者和編輯者
 - 何時與他人共用
- ✓ 變更檔案權限或刪除檔案

[說明中心相關文件](#)

[適用於雲端硬碟記錄事件的條件](#) [適用於雲端硬碟記錄事件的動作](#)

“

有人不小心與其他群組共用了某個檔案，而這個群組不該擁有該檔案的存取權。我要移除該群組的檔案存取權。”

[逐步操作說明](#)

不小心共用檔案

調查工具中的雲端硬碟記錄可協助您追蹤和解決檔案共享問題。

存取[雲端硬碟記錄](#)可讓您：

- ✓ 根據名稱、執行者和擁有者等條件搜尋文件
- ✓ 查看該文件的所有記錄資訊，包括檢視過檔案的對象和檔案共用的時間點
- ✓ 變更檔案權限和停用下載、影印與複製功能

[說明中心相關文件](#)

[適用於雲端硬碟記錄事件的條件](#) [適用於雲端硬碟記錄事件的動作](#)

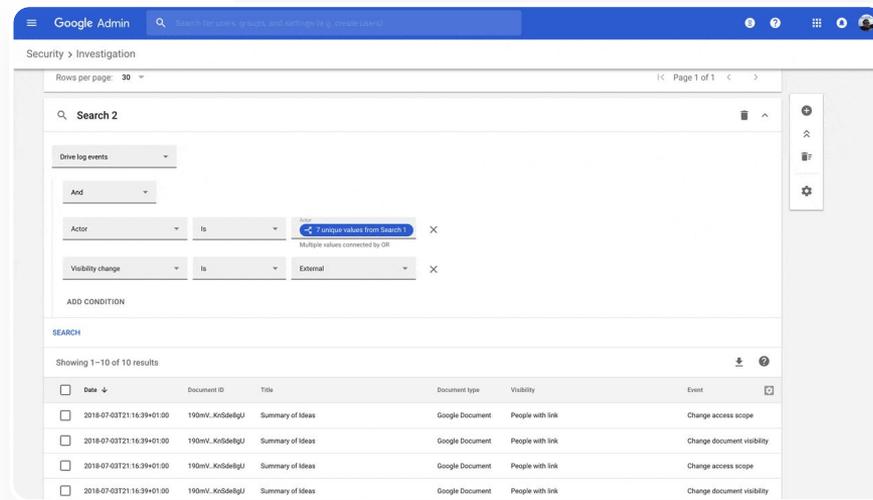
操作說明：雲端硬碟記錄事件

如何調查

- 登入管理控制台
- 依序點選「安全性」>「調查工具」
- 選擇「雲端硬碟記錄事件」
- 依序點選「新增條件」>「搜尋」

如何採取行動

- 在搜尋結果中選取相關檔案
- 依序點選「動作」>「稽核檔案權限」，即可開啟「權限」頁面
- 點選「使用者」來查看誰擁有存取權
- 按一下「連結」查看或修改所選檔案的連結共用設定
- 按一下「待處理的變更」檢查變更內容，然後儲存變更



[說明中心相關文件](#)

[適用於雲端硬碟記錄事件的條件](#)

[適用於雲端硬碟記錄事件的動作](#)

“

有人傳送了不該傳送的電子郵件。
我們想知道收件者是誰、對方是否已
開啟或回覆郵件，並刪除這封電子郵
件。我也想知道電子郵件的內容。”

[逐步操作說明](#)

電子郵件分類

調查工具中的Gmail 記錄能協助您找出網域中具有危險或不當的電子郵件並採取行動。存取 Gmail 記錄可讓您：

- ✓ 根據主旨、郵件 ID、附件、寄件者等條件搜尋特定電子郵件。
- ✓ 查看電子郵件詳細資料，包括作者、收件者、開啟和轉寄情形。
- ✓ 根據搜尋結果執行動作。使用者可針對 Gmail 郵件採取的動作包括刪除、還原、標記為垃圾郵件或網路詐騙，以及傳送至收件匣或隔離區。

[🔗 說明中心相關文件](#)[適用於 Gmail 記錄和
Gmail 郵件的條件](#)[適用於 Gmail 郵件和
Gmail 記錄事件的動作](#)[查看電子郵件內容
所需步驟](#)

網路詐騙和惡意軟體電子郵件

您可使用調查工具中的 Gmail 記錄找出並隔離網域中的惡意電子郵件。存取 Gmail 記錄可讓您：

- ✓ 根據特定內容和附件搜尋電子郵件
- ✓ 查看郵件和會話串，判斷郵件是否帶有不當企圖
- ✓ 查看特定電子郵件的資訊，包括收件者和開啟狀態
- ✓ 將郵件標記為垃圾郵件或詐騙郵件、傳送至特定收件匣或隔離區，或是刪除郵件

[🔗 說明中心相關文件](#)

[適用於 Gmail 記錄和 Gmail 郵件的條件](#)

[適用於 Gmail 郵件和 Gmail 記錄事件的動作](#)

[查看電子郵件內容所需步驟](#)



使用者收到一封疑似是網路詐騙或惡意軟體的電子郵件。我們想知道使用者是否有點擊郵件中的連結或下載附件，因為這麼做可能會讓使用者和我們的網域遭受危害。”

[逐步操作說明](#)

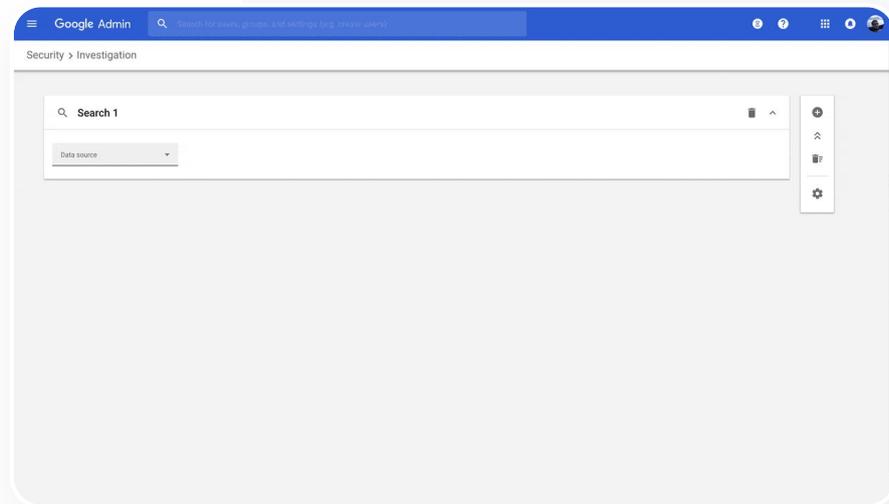
操作說明：Gmail 記錄

如何調查

- 登入管理控制台
- 依序點選「安全性」>「調查工具」
- 選擇「Gmail 記錄事件」或是「Gmail 郵件」
- 依序點選「新增條件」>「搜尋」

如何採取行動

- 在搜尋結果中選取相關郵件
- 按一下「動作」
- 選取「刪除收件匣中的郵件」
- 按一下「從收件匣中刪除」
- 如要確認此動作，請點選頁面底端的「查看」
- 您可在「結果」欄中查看動作狀態



[🔗 說明中心相關文件](#)

[適用於 Gmail 記錄和 Gmail 郵件的條件](#)

[適用於 Gmail 郵件和 Gmail 記錄事件的動作](#)

[查看電子郵件內容所需步驟](#)

“

有惡意行為人不斷嘗試駭入網域中重要的使用者帳戶，我卻怎麼樣都抓不到他們。我要怎麼遏止這個情況？”

[逐步操作說明](#)

阻止不肖人士

調查工具中的使用者記錄可協助您：

- ✓ 辨識嘗試入侵貴機構使用者帳戶的行為，並進行調查
- ✓ [使用調查工具建立活動規則](#)：自動封鎖來自特定執行者的郵件或其他惡意活動
- ✓ 監控貴機構使用者正在使用的兩步驟驗證方式
- ✓ [透過進階保護計畫](#)，進一步保護重要的使用者帳戶
- ✓ 進一步瞭解貴機構使用者登入失敗的情況
- ✓ 還原使用者或將使用者停權

[說明中心相關文件](#)[搜尋及調查使用者記錄事件](#)[使用調查工具建立活動規則](#)

操作說明：使用者記錄事件

如何調查

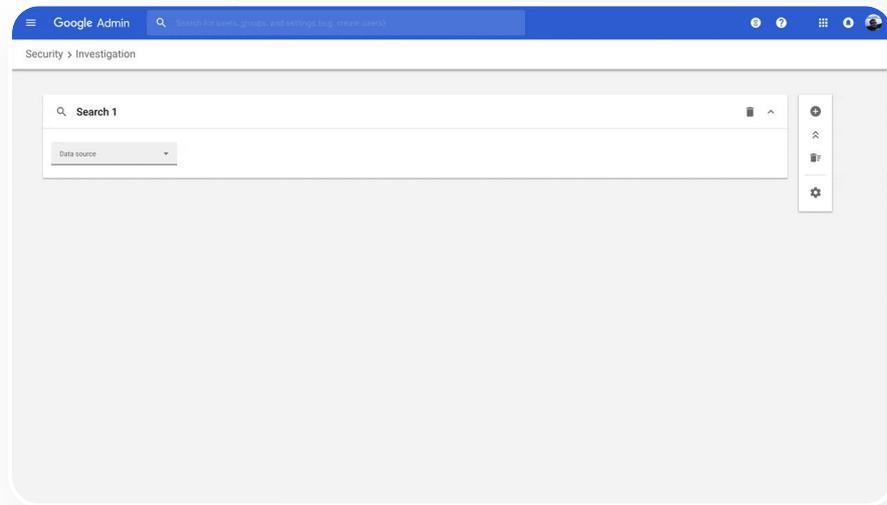
- 登入管理控制台
- 依序點選「安全性」>「調查工具」
- 選擇「使用者記錄事件」
- 依序點選「新增條件」>「搜尋」

如何還原使用者或將使用者停權

- 在搜尋結果中選取一或多位使用者
- 點選「動作」下拉式選單
- 按一下「還原使用者」或「將使用者停權」

如何查看特定使用者的詳細資料

- 在搜尋結果頁面上選取一位使用者
- 然後在「動作」下拉式選單中點選查看詳細資料



[🔗 說明中心相關文件](#)

[搜尋及調查使用者記錄事件](#)

🔒 安全性資訊主頁

這是什麼？

使用安全性資訊主頁即可查看各項安全性報告總覽。根據預設，每個安全性報告面板都會顯示最近 7 天的資料。您可以為資訊主頁自訂顯示的資料時間範圍，例如「今天」、「昨天」、「本週」、「上週」、「本月」、「上個月」或「幾天前」(最多 180 天)。

用途

大量垃圾郵件



[逐步操作說明](#)

對外共用檔案



[逐步操作說明](#)

第三方應用程式

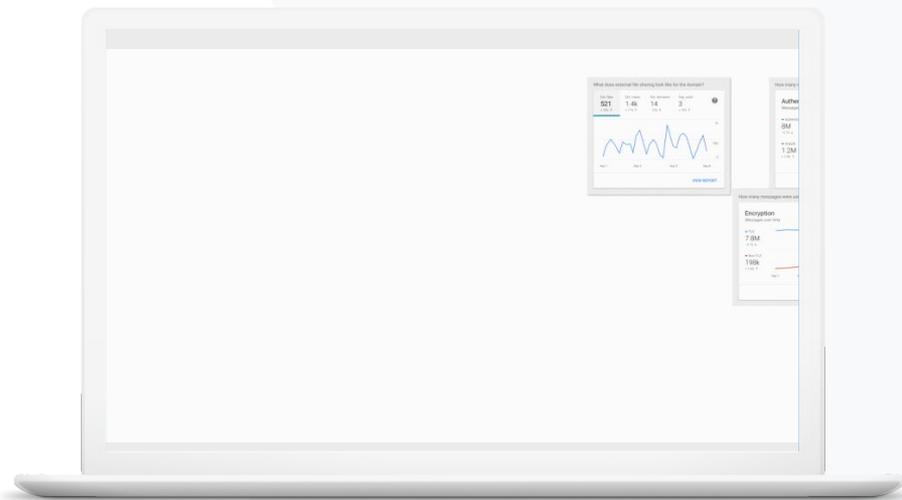


[逐步操作說明](#)

網路詐騙



[逐步操作說明](#)



“

我想控管過多且不必要的電子郵件，並減少學校受到的安全性威脅。”

[逐步操作說明](#)

大量垃圾郵件

安全性資訊主頁以圖表方式呈現 Google Workspace for Education 環境中各項活動狀態，包括：

- ✓ 垃圾內容
- ✓ 可疑附件
- ✓ 網路詐騙
- ✓ 其他
- ✓ 惡意軟體

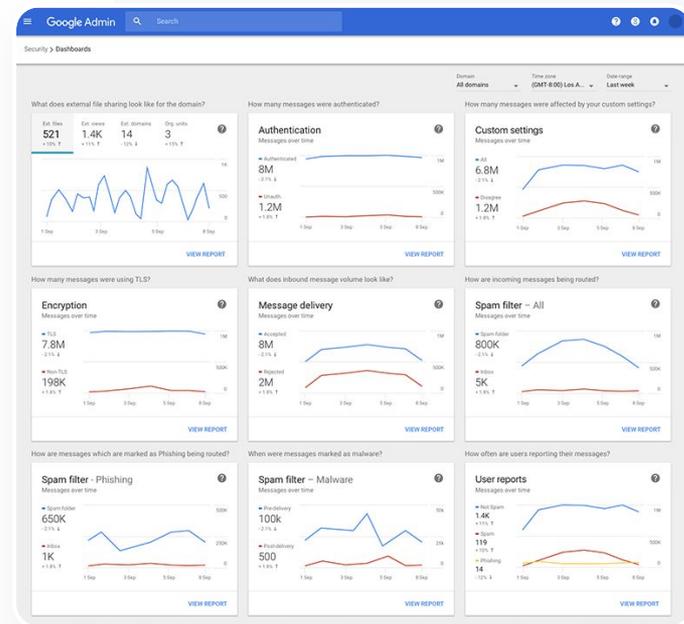
[說明中心相關文件](#)

[關於安全性資訊主頁](#)

操作說明：資訊主頁總覽

如何查看資訊主頁

- 登入管理控制台
- 依序點選「安全性」>「資訊主頁」
- 您可透過安全性資訊主頁深入瞭解資料、將資料匯出至試算表或第三方工具，或是在調查工具中展開調查



[說明中心相關文件](#)

[關於安全性資訊主頁](#)

“

我想查看檔案對外共用的活動，
防止機密資料外洩至第三方。”

[逐步操作說明](#)

對外共用檔案

使用安全性資訊主頁中的檔案公開報告，即可查看貴機構網域中的對外共用檔案指標，包括：

- ✓ 在特定時間範圍內與外部使用者共用檔案的事件次數
- ✓ 對外共用檔案在特定時間範圍內被檢視的次數

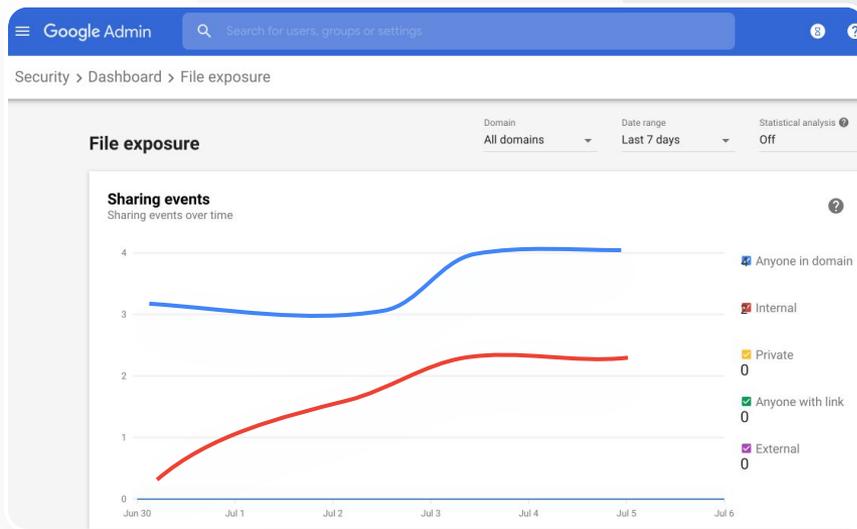
[說明中心相關文件](#)

[開始使用安全性狀態頁面](#)

操作說明：檔案公開報告

如何查看報告

- 登入管理控制台
- 依序點選「安全性」>「資訊主頁」
- 在命名為這個網域的外部檔案共用狀態為何？的資訊面板中，點選右下角的「查看報告」



[🔗 說明中心相關文件](#)

[關於安全性資訊主頁檔案公開報告](#)



“

我想查看有哪些第三方應用程式能存取我網域中的資料。”

[逐步操作說明](#)

第三方應用程式

使用安全性資訊主頁中的 OAuth 授權活動報告，即可監控連結至貴機構網域的第三方應用程式，以及這些應用程式可存取的資料。



OAuth 可在不揭露使用者密碼的情況下，授權第三方服務存取使用者的帳戶資訊。您可能會想限制擁有存取權的第三方應用程式。



使用 OAuth 授權活動面板並根據應用程式、範圍或使用者來監控授權活動，並更新授予權限。



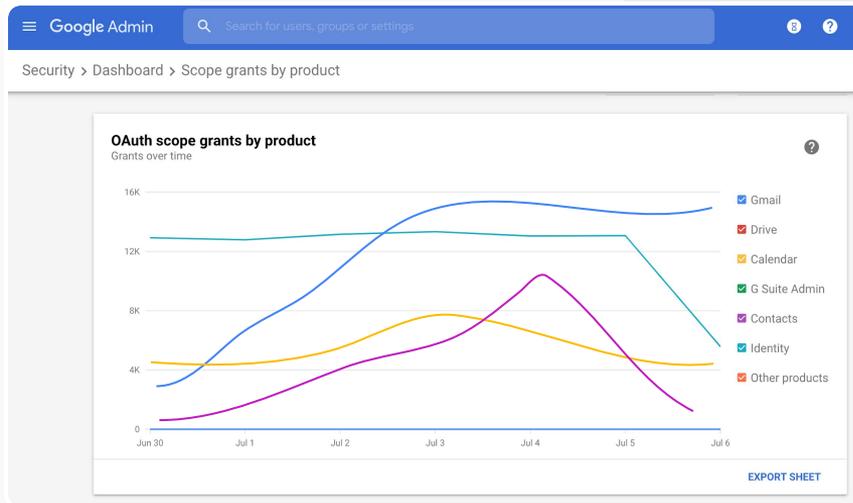
[說明中心相關文件](#)

[OAuth 授權活動報告](#)

操作說明：OAuth 授權活動報告

如何查看報告

- 登入管理控制台
- 依序點選「安全性」>「資訊主頁」
- 按一下底部的「查看報告」
- 您可根據產品（應用程式）、範圍或使用者查看 OAuth 授權活動
- 如要篩選資訊，請點選「應用程式」、「範圍」，或「使用者」
- 如要根據這份報告產生試算表，請點選「匯出試算表」



[🔗 說明中心相關文件](#)

[OAuth 授權活動報告](#)

“

有使用者回報收到網路詐騙電子郵件。我想追蹤他們收到這封郵件的時間、郵件的性質，以及使用者會面臨的風險。”

[逐步操作說明](#)

網路詐騙

使用安全性資訊主頁中的「使用者回報」面板，即可查看在特定時間範圍內被標記為網路詐騙或垃圾郵件的電子郵件。您可查看被標記為網路詐騙的電子郵件資訊，例如收件者與開啟情形。

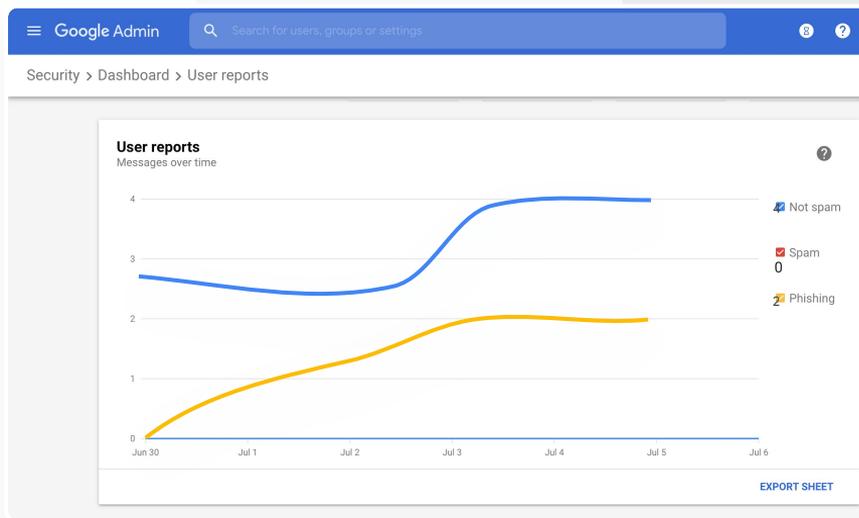
- ✓ 使用者回報可讓您查看使用者在特定的時間範圍內標示郵件 (垃圾郵件、非垃圾郵件或網路詐騙郵件) 的情況
- ✓ 您可以自訂圖表，以便查看特定電子郵件類型的詳細資料，例如由內部或外部網域傳送，或傳送的日期範圍等

[說明中心相關文件](#)[使用者如何標示電子郵件？](#)[使用者回報](#)

操作說明：使用者回報面板

如何查看報告

- 登入管理控制台
- 依序點選「安全性」>「資訊主頁」
- 在「使用者回報」面板右下角，按一下「查看報告」



[🔗 說明中心相關文件](#)

[關於安全性資訊主頁檔案公開報告](#)

安全性狀態

這是什麼？

安全性狀態頁面提供 Google Workspace 環境中的安全防護設定總覽，可讓您比較現有設定和 Google 的建議設定，以便主動為機構提供保護。

用途

[針對風險區域的建議做法](#)



[逐步操作說明](#)

[即時掌握最佳做法](#)



[逐步操作說明](#)

[安全性最佳做法](#)

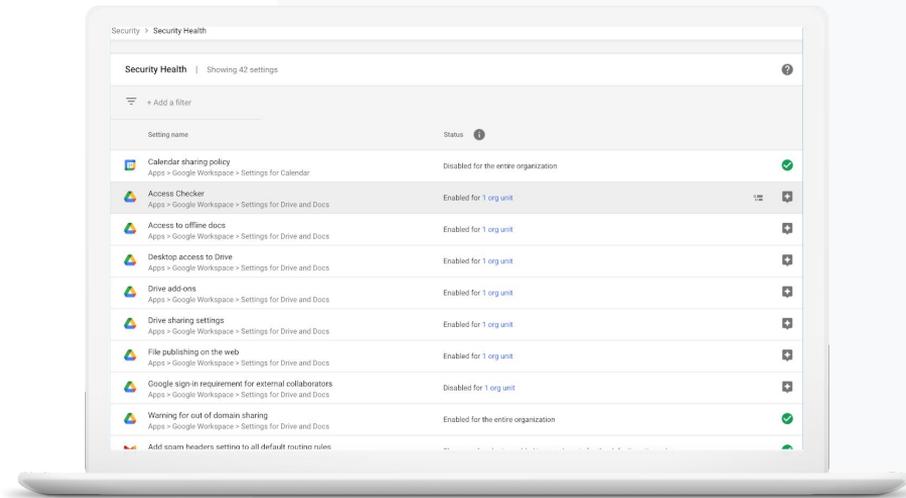


[逐步操作說明](#)

[為人數漸增的學校提升安全性](#)



[逐步操作說明](#)



“

我想取得網域安全性設定的數據匯報摘要和可採取的設定建議，好修正具有潛在風險的區域。”

[逐步操作說明](#)

針對風險區域的建議做法

安全性狀態頁面可用來檢查安全性設定並標記出建議變更的設定。

您可透過安全性狀態頁面執行以下操作：

- ✓ 快速辨識網域中具有潛在風險的區域
- ✓ 取得最佳化設定建議，提高機構的安全性成效
- ✓ 在安全性建議頁面中查看額外資訊及支援文章

[說明中心相關文件](#)

[開始使用安全性狀態頁面](#)

“

我負責管理機構網域，但我無法掌握所有情況。請協助我採用正確的設定，確保所有資料安全無虞。”

[逐步操作說明](#)

即時掌握最佳做法

安全性狀態頁面可用來檢查安全性設定並標記出建議變更的設定。

您可透過安全性狀態頁面獲得下列項目：

- ✓ 針對網域中潛在風險區域提供的建議
- ✓ 可提高安全性成效的最佳化設定建議
- ✓ 額外資訊與支援文章

[說明中心相關文件](#)

[開始使用安全性狀態頁面](#)

安全性最佳做法

開啟安全性狀態頁面，即可接收下列安全性政策最佳做法：

- ✓ 針對網域中潛在風險區域提供的建議
- ✓ 可提高安全性成效的最佳化設定建議
- ✓ 直接前往設定的連結
- ✓ 額外資訊與支援文章

[說明中心相關文件](#)

[開始使用安全性狀態頁面](#)

“

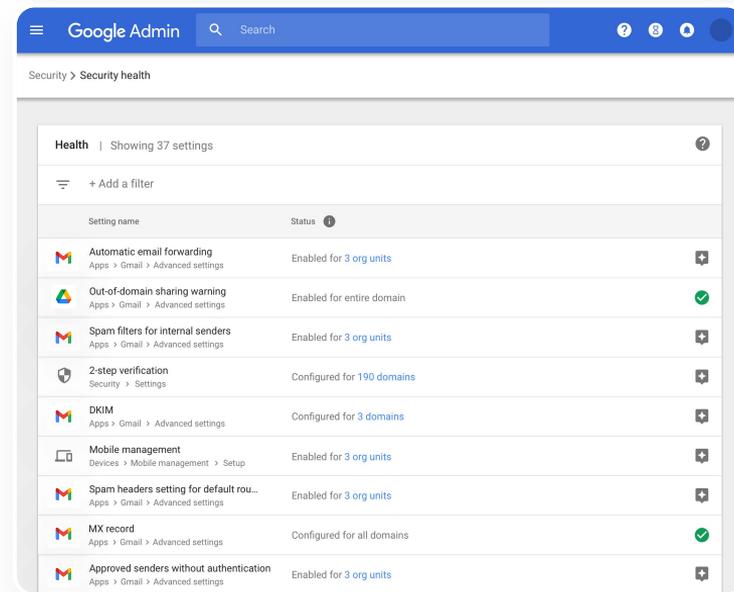
請引導我採用最佳做法，或是提供安全性政策的設定建議。”

[逐步操作說明](#)

操作說明：安全性建議

如何查看建議

- 登入管理控制台
- 依序點選「安全性」>「安全性狀態」
- 查看最右側欄的狀態設定
 - 顯示綠色勾號即表示設定安全無虞
 - 顯示灰色圖示表示系統建議您進一步檢查設定；只要按一下圖示即可開放詳細資料和操作說明



[說明中心相關文件](#)

[開始使用安全性狀態頁面](#)

“

校內的教職員和學生人數不斷增加，我想盡可能確保學校資料安全無虞。”

[逐步操作說明](#)

為人數漸增的學校提升安全性

IT 管理員應遵循這些[安全性最佳做法](#)，強化公司的資安與隱私防護能力。您可使用 Google 管理控制台中的一或多項設定，來落實檢查清單中的最佳做法。

- ✔ 防止和解決帳戶被盜的建議設定
- ✔ 限制與網域外使用者共用和協作的步驟
- ✔ 可用來檢查第三方應用程式是否能存取核心服務的功能

[說明中心相關文件](#)

[適用於中大型企業的安全性檢查清單](#)

操作說明：安全性檢查清單

為保護貴機構的資料，Google 預設會按照這份檢查清單所列的安全性最佳做法啟用多項建議設定。建議您進一步查看下列項目的詳細說明。

- 管理員：保護管理員帳戶
- 帳戶：防止帳戶被盜及相關因應措施
- 應用程式：檢查第三方應用程式的核心服務存取權
- 日曆：限制日曆外部共用設定
- 雲端硬碟：限制與網域外使用者的共用和協作活動
- Gmail：設定驗證和基礎架構
- 保管箱：控管、稽核保管箱帳戶並確保安全

Security best practices

To help protect your business, Google turns on many of the settings recommended in this checklist as security best practices by default.

[Administrator](#) | [Accounts](#) | [Apps](#) | [Calendar](#) | [Chrome Browser and Chrome OS](#) | [Classic Hangouts](#)
[Contacts](#) | [Drive](#) | [Gmail](#) | [Google+](#) | [Groups](#) | [Mobile](#) | [Sites](#) | [Vault](#)

Administrator ^

Protect admin accounts

- Require 2-Step Verification for admin accounts**
Because super admins control access to all business and employee data in the organization, it's especially important for their accounts to be protected by an additional authentication factor.

[Protect your business with 2-Step Verification](#) | [Deploy 2-Step verification](#)

- Use security keys for 2-Step Verification**
Security keys help to resist phishing threats and are the most phishing-resistant form of 2-Step Verification.

[Protect your business with 2-Step Verification](#)

[🔗 說明中心相關文件](#)

[🔒 監控安全性設定狀態](#)

進階管理控制項

這是什麼？

監控和控制可存取機構網域和資料的使用者及裝置。

用途

[資料相關法規](#)



[逐步操作說明](#)

[授權相關法規](#)



[逐步操作說明](#)

[應用程式限制](#)



[逐步操作說明](#)

[管理行動裝置](#)

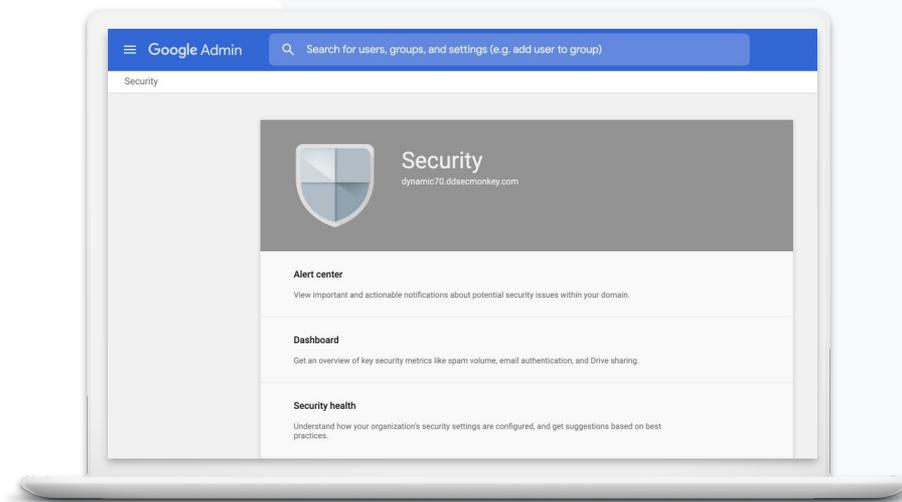


[逐步操作說明](#)

[遷移資料](#)



[逐步操作說明](#)





資料相關法規

資料地區政策可讓管理員選擇將資料存放在美國或英國/歐洲等特定地理位置。

“

根據法規，我校內學生和教職員的資料必須存放在美國。”

- ✔ 您可以為部分使用者選擇單一資料地區，也可以為特定部門或團隊選擇不同資料地區
- ✔ 將使用者加入依部門設定的機構單位，或是加入可包含不同部門使用者的配置群組
- ✔ 資料地區政策不適用於不具備 Education Standard 或 Education Plus 授權的使用者



[說明中心相關文件](#)

[選擇資料存放的地理位置](#)

[逐步操作說明](#)

“

根據授權法規，我機構內的
研究資料必須存放在美國
境內。”

[逐步操作說明](#)

授權相關法規

資料地區政策可讓管理員選擇將機構的研究資料存放在特定地理位置 (美國或歐洲)。

- ✓ 資料地區政策適用於多數 Google Workspace for Education 核心服務的主要靜態資料 (包括備份資料)，若要查看資料清單，請點選[這裡](#)
- ✓ 如果使用者不在資料存放的地區，有時會經歷較長的延遲時間，因此在設定資料地區政策前請先評估損益

[🔗 說明中心相關文件](#)

[選擇資料存放的地理位置](#)

操作說明：資料地區*

如何指定資料地區

- 登入管理控制台
 - 注意：必須以超級管理員的身分登入，才能進行設定。
- 依序點選「公司設定檔」>「顯示更多」>「資料地區」
- 選取要限制地區的機構單位或配置群組，或是選取整欄以涵蓋所有單位和群組
- 選取地區，選項包括無偏好設定、美國或歐洲
- 按一下「儲存」

*只有使用 Education Standard 或 Education Plus 的機構能使用資料地區功能，將資料存放在特定地區。

[🔗 說明中心相關文件](#)

[選擇資料存放的地理位置](#)

“

我想限制使用者在網路上對特定應用程式的存取權。”

[逐步操作說明](#)

應用程式限制

只要使用情境感知存取權*，您就能根據使用者身分、位置、裝置安全性狀態和 IP 位址等屬性，為應用程式建立精準的存取權控管政策。您還可以禁止透過外部網路存取應用程式。

- ✓ 您可以將情境感知存取權政策套用至 Google Workspace for Education 的核心服務
- ✓ 舉例來說，如果使用者在校內登入 Google Workspace 的核心服務，隨後前往咖啡廳，則系統會在使用者的位置變更時，重新檢查服務的情境感知存取權政策

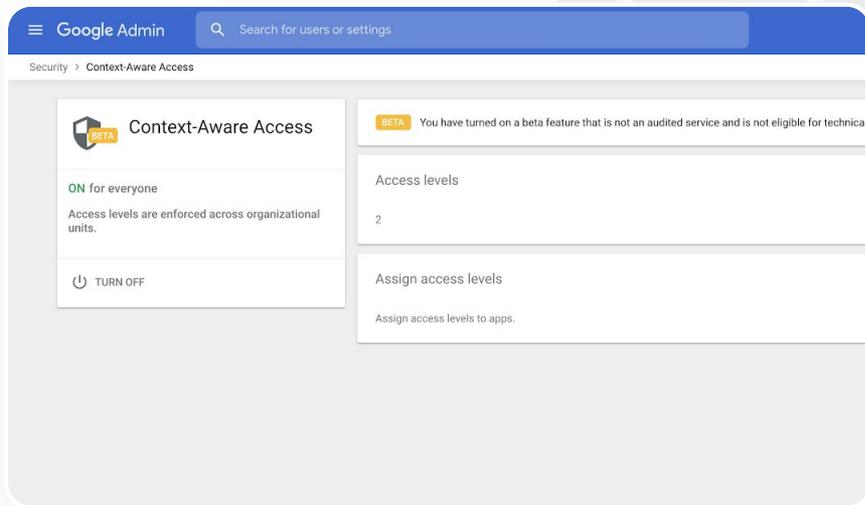
[🔗 說明中心相關文件](#)[情境感知存取權總覽](#)[為應用程式指派情境感知存取權層級](#)

*情境感知存取權政策僅適用於使用 Education Standard 或 Education Plus 的機構。

操作說明：情境感知存取權

如何使用情境感知存取權

- 登入管理控制台
- 依序選取「安全性」>「情境感知存取權」>「指派」
- 選取「指派存取層級」即可查看應用程式清單
- 選取「機構單位或配置群組」來排序清單
- 在要調整的應用程式旁，選取「指派」
- 選取一或多個存取層級
- 如要讓使用者符合多個條件，請建立多個層級
- 按一下「儲存」



[說明中心相關文件](#)

[情境感知存取權總覽](#)

[為應用程式指派情境感知存取權層級](#)



管理行動裝置

使用進階行動管理可讓您透過行動裝置進一步控管機構資料。您可以對行動裝置功能設定限制、要求加密保護裝置、管理 Android 裝置、iPhone 和 iPad 上的應用程式，以及抹除裝置資料。



您可以透過管理控制台核准、封鎖、解除封鎖或刪除裝置。



若是有成員遺失裝置或遭到學校退學，您可以從特定的管理模組裝置上抹除使用者的帳戶、個人設定檔，甚至是所有資料。該資料仍會出現在電腦或網路瀏覽器上。



說明中心相關文件

[設定進階行動管理服務](#)

[核准、封鎖、解除封鎖或刪除裝置](#)

[移除裝置上的資料](#)

“

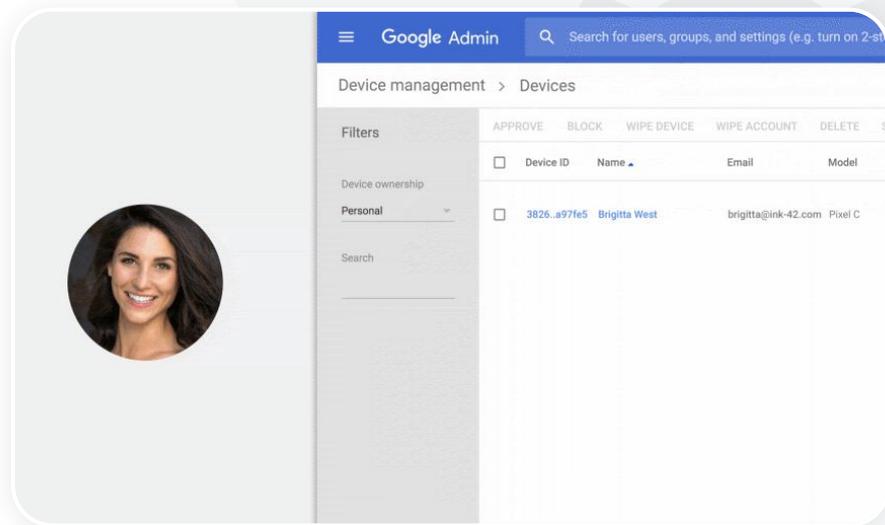
我需要管理學區內所有類型的裝置，包括 Chromebook、iOS 和 Windows 10 等裝置，並統一套用相同的政策，尤其是裝置遭駭時，就更需要這樣的功能。”

[逐步操作說明](#)

操作說明：啟用進階行動管理服務

如何啟用

- 登入管理控制台。
- 依序前往「管理控制台」>「裝置」。
- 點選左側的「設定」>「通用設定」。
- 依序點選「一般」>「行動管理服務」。
- 如要為所有使用者套用設定，請選取頂層機構單位；否則請選取子機構單位。
- 選取「進階」。
- 按一下「儲存」。



[🔗 說明中心相關文件](#)

[設定進階行動管理服務](#)

[核准、封鎖、解除封鎖或刪除裝置](#)

[移除裝置上的資料](#)



遷移資料

使用遷移指南即可將整個機構的資料移動至 Google Workspace，例如電子郵件、日曆、聯絡人、資料夾、檔案和權限設定。

少於 1,000 位使用者的資料

- ✓ 查看產品對照表，瞭解哪項解決方案最能滿足貴機構的需求。

[瞭解詳情](#)

多於 1,000 位使用者的資料

- ✓ 使用 Google Workspace Migrate 可確保有效遷移大量資料。

[瞭解詳情](#)

[🔗 說明中心相關文件](#)

[將貴機構的資料遷移至 Google Workspace](#)

[Google Workspace 遷移產品對照表](#)

[關於 Google Workspace Migrate](#)

[安裝及設定 Google Workspace Migrate](#)



我們要改用 Google Workspace，因此需要將所有資料遷移至新的 Google 環境。”

[逐步操作說明](#)

操作說明：Google Workspace Migrate

事前準備

註冊 [Beta 版](#)，確保您符合 [系統需求](#)。

操作說明

1. 設定 Google Cloud Console

[啟用 API](#)

[建立 OAuth 網路用戶端 ID](#)

[建立 Google Workspace 服務帳戶](#)

2. 設定管理控制台

[設定管理員角色](#)

[授權用戶端 ID](#)

3. 下載及安裝

[下載安裝程式](#)

[安裝資料庫](#)

[安裝及設定平台](#)

[安裝節點伺服器](#)

[\(選用\) 將節點伺服器設為使用傳輸層](#)

[安全標準 \(TLS\)](#)

4. 設定遷移產品

[設定加密金鑰](#)

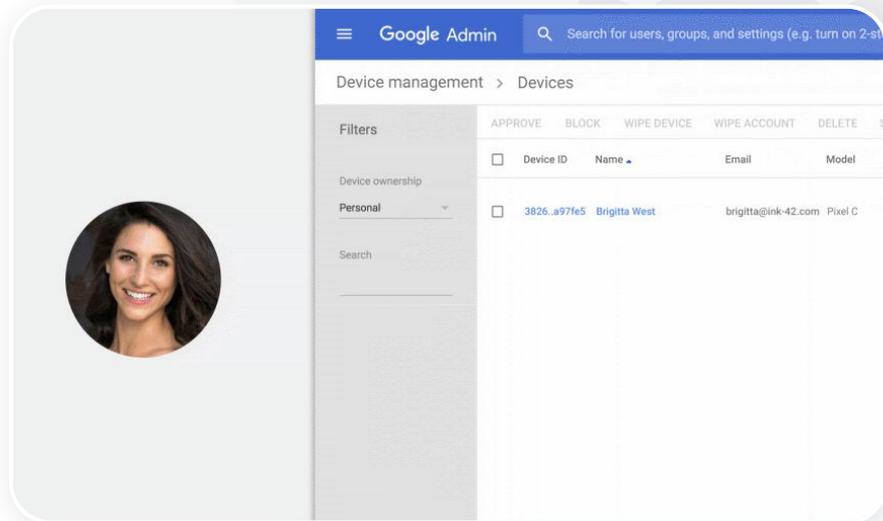
[調整資料庫設定](#)

[設定回呼網址](#)

[新增節點伺服器](#)

[建立專案](#)

需要協助嗎？請聯絡 [Google Cloud Partner](#)。



[說明中心相關文件](#)

[關於 Google Workspace Migrate](#)

[安裝及設定 Google Workspace Migrate](#)

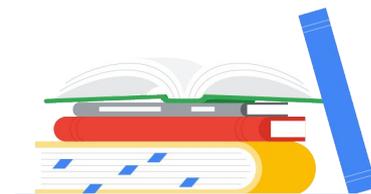
[將貴機構的資料遷移至 Google Workspace](#)

[Google Workspace 遷移產品對照表](#)



教學與學習工具

透過更強大的視訊溝通服務、豐富的課程體驗，以及可促進學術誠信的各项工具，讓貴機構的教育工作者在數位學習環境中享有更多功能。



[原創性報告](#)



[Google Meet](#)

原創性報告

這是什麼？

教育工作者和學生可以檢查作業是否涉嫌抄襲。原創性報告會運用 Google 搜尋服務，將學生的作業與數十億個網頁和數百萬本書籍進行比較，然後提供偵測到的網頁連結，並標記未註明引用出處的文字。

用途

偵測抄襲內容

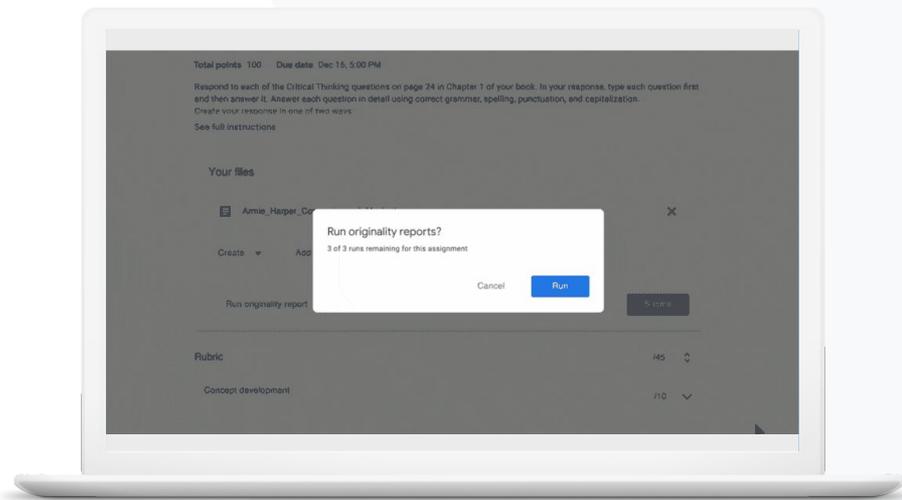


[逐步操作說明](#)

將抄襲偵測功能變成學習機會



[逐步操作說明](#)



“

我想檢查學生的作業是否涉嫌抄襲或含有不正確的引用出處。”

[逐步操作說明](#)

偵測抄襲內容

原創性報告可以讓老師檢查學生的作業是否涉嫌抄襲。原創性報告會運用 Google 搜尋服務，將學生的作業與數十億個網頁和數百萬本書籍進行比較。

- ✓ 使用 Teaching and Learning Upgrade 或 Education Plus 的教育工作者可無限次產生原創性報告
- ✓ 原創性報告功能目前僅適用於：
 - 語言設定為英文的 Google 帳戶
 - 使用 Google 文件完成的作業
 - Google for Education 帳戶

[說明中心相關文件](#)

[開啟原創性報告功能](#)

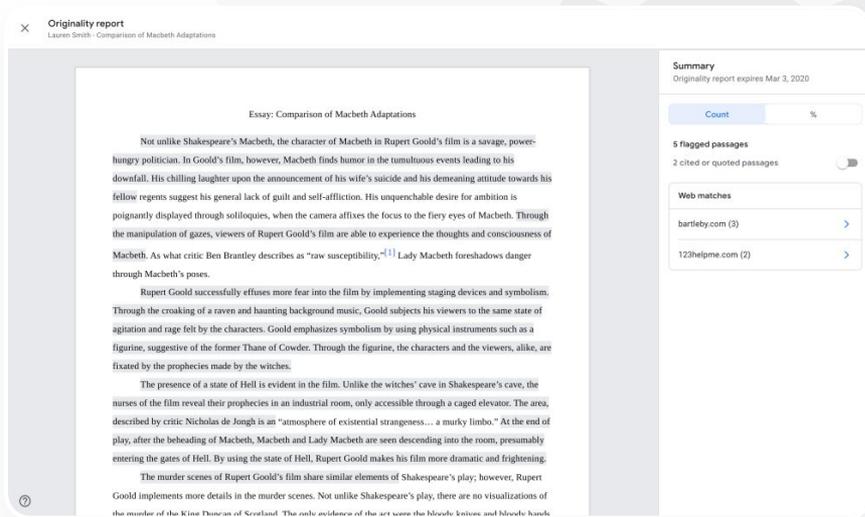
操作說明：教育工作者後續檢查

如何為作業開啟原創性報告

- 透過 classroom.google.com 登入 Classroom 帳戶
- 從清單中選取相關課程，並選擇「課堂作業」
- 依序選取「建立」>「作業」
- 勾選「原創性報告」旁的方塊來啟用報告

如何針對學生作業產生原創性報告

- 從清單中選取學生的檔案，按一下即可在評分工具中開啟檔案
- 在學生的作業下方點選「檢查原創性」



[說明中心相關文件](#)

[開啟原創性報告功能](#)

將抄襲偵測功能變成學習機會

“

我想讓學生自行檢查作業是否涉嫌抄襲，並將這個作弊偵測功能變成他們的學習機會。”

學生在繳交每份作業前，最多可產生 3 次原創性報告，以便找出未註明引用出處和無意中抄襲的內容。原創性報告功能會針對各個來源比對學生的文件，並標記未引用出處的文字，藉此讓學生有機會學習、修正錯誤，並在繳交作業時更有自信。

- ✓ 使用 Teaching and Learning Upgrade 和 Education Plus 的教育工作者皆可產生無限次原創性報告，Education Fundamentals 的使用者則只能針對每堂課啟用 5 次報告。
- ✓ 學生繳交作業後，Classroom 會自動產生一份只有老師才能查看的報告。如果學生將作業取消繳交後再重新繳交，Classroom 會為老師建立另一份原創性報告。

[逐步操作說明](#)

[說明中心相關文件](#)

[針對作業產生原創性報告](#)

操作說明：學生事前檢查

學生如何產生原創性報告

- 透過 classroom.google.com 登入 Classroom 帳戶
- 從清單中選取相關課程，並選擇「課堂作業」
- 選取清單中的相關作業，並點選「查看作業」
- 在「你的作業」下方，選取「上傳」或「建立檔案」
- 按一下「原創性報告」旁邊的「執行」
- 如要開啟報告，請點選檔案作業名稱下方的「查看原創性報告」
- 如要修改作業或是為標記的段落提供正確引用出處，請按一下底部的「編輯」

Essay: Comparison of Macbeth adaptations

Not unlike Shakespeare's Macbeth, the character of Macbeth in Rupert Goold's film is a savage, power-hungry politician. In Goold's film, however, Macbeth first hovers in the limbo between reality and his downfall. His chilling laughter upon announcement of his wife's suicide and his demeaning attitude towards his fellow agents suggest his general lack of guilt and self-affliction. His unquenchable desire for ambition is poignantly displayed through soliloquies, when the camera affixes the focus to the fiery eyes of Macbeth. Through the manipulation of gases, viewers of Rupert Goold's film are able to experience the thoughts and consciousness of Macbeth. As what critic Ben Brantley describes as "raw susceptibility," Lady Macbeth foreshadows danger through Macbeth's poses.

Rupert Goold successfully effuses more fear into the film by implementing staging devices and symbolism. Through the croaking of a raven and haunting background music, Goold subjects his viewers to the same state of agitation and rage felt by the characters. Goold emphasizes symbolism by using physical instruments such as a figurine, suggestive of the former Thane of Cowdrie. Through the figurine, the characters and the viewers, alike, are fixated by the prophecies made by the witches.

The presence of a state of Hell is evident in the film. Unlike the witches' cave in Shakespeare's play, the nurses of the film reveal their prophecies in an industrial room, only accessible through a caged elevator. The area, described by critic Nicholas de Jongh is an "atmosphere of existential strangeness... a murky limbo." At the end of play, after the beheading of Macbeth, Macbeth and Lady Macbeth are seen descending into the room, presumably entering the gates of Hell. By using the state of Hell, Rupert Goold makes his film more dramatic and frightening.

The murder scenes of Rupert Goold's film share similar elements of Shakespeare's play; however, Rupert Goold implements more details in the murder scenes. Not unlike Shakespeare's play, there are no visualizations of the murder of the King Duncan of Scotland. The only evidence of the act were the bloody knives and bloody hands of Macbeth used in the execution. Unlike Shakespeare's play, the murder of Banquo occurs in a public setting. By having the execution of Banquo on a train, Goold stresses the power and boldness of Macbeth.

Through his film, Goold introduces an element of absurdity to several scenes. Before the murder of Banquo, Rupert Goold

Web matches > sparksnotes.com ✕

STUDENT'S PASSAGE

Many of Shakespeare's plays were published in editions of **varying quality and accuracy in his lifetime. However, in 1623, two fellow actors and friends of Shakespeare's**, John Heminges and Henry Condell, published a more definitive text

[Comment](#)

TOP MATCH

Of my favorite plays there is inconsistency, illustrating **varying quality and accuracy in his lifetime. However, in 1623, two fellow actors and friends of Shakespeare's**, developed a new way to translate and preserve the content language

SparksNotes - Macbeth Act III: The return of Macb...
<http://sparksnotes.macbethingstoreadthataveryimportant...>

[🔗 說明中心相關文件](#)

[針對作業產生原創性報告](#)

Google Meet

這是什麼？

Google Meet 的進階功能包括直播、分組討論室、將會議錄製內容儲存至雲端硬碟、出席狀況報告，以及發起最多可讓 250 人參與的會議等。

用途

安全的視訊會議



[逐步操作說明](#)

提高視訊會議安全性



[逐步操作說明](#)

錄製課程



[逐步操作說明](#)

錄製教職員會議



[逐步操作說明](#)

錯過的課程



[逐步操作說明](#)

直播會議



[逐步操作說明](#)

直播學校活動



[逐步操作說明](#)

提出問題



[逐步操作說明](#)

收集意見



[逐步操作說明](#)

學生小組



[逐步操作說明](#)

追蹤出席狀況



[逐步操作說明](#)

安全的視訊會議

有了 Google Meet，學校就能充分運用 Google 用來保護個人資訊和隱私的各項功能，包括內建防護機制、全球網路，以及融入安全性考量所設計的基礎架構。下列

Google Meet 安全措施值得您的信賴：

- ✔ 隱私權和法規遵循遵循嚴格的教育安全性標準，進一步保障學生和學校資料安全
- ✔ 加密：Google 會將客戶的所有資料進行加密
- ✔ 反濫用措施：讓主持人控制出席狀況，確保只有相關人員加入會議
- ✔ 安全的部署、存取與控管機制：提供多項預防措施，保護會議的私密性與安全性
- ✔ 事件回應機制：Google 整體安全性與隱私權計畫的一大面向，同時也是遵循全球隱私權規範的關鍵
- ✔ 穩定性：多層式的雲端原生基礎架構易於擴充，且可應付用量暴增的情況
- ✔ 控管參與者：改版的傳送加入要求功能可讓符合特定條件的使用者大量管理和封鎖加入要求
- ✔ 鎖定控制項：主持人可以控管誰能在虛擬會議期間傳送即時通訊訊息、分享螢幕畫面或是發言

[逐步操作說明](#)

提高視訊會議安全性

Teaching and Learning Upgrade 和 Education Plus 提供額外的反濫用措施，包括外部參與者必須經過核准、更完善的會議管理控制項，以及已設定暱稱的會議，藉此防止參與者重複加入已結束的會議。最後一位參與者離開會議後，參與者就無法重新加入會議。在老師重新發起已設定暱稱的會議之前，學生將無法再次加入。

- ✓ 若發起已設定暱稱的會議，最後一位參與者離開會議後，參與者便無法重新加入，10 位數的會議代碼也會失效
- ✓ 在老師重新發起已設定暱稱的會議前，學生將無法再次加入
- ✓ 老師可以為所有參與者結束會議，防止參與者在老師離開後繼續留在會議中

[🔗 說明中心相關文件](#)

[與教育相關的 Meet 安全性與隱私權資訊](#)

[發起 Google Meet 視訊會議](#)



我要如何提高校內視訊會議的安全性？”

[逐步操作說明](#)

操作說明：已設定暱稱的會議

如何建立已設定暱稱的會議

- 使用短連結，例如 [g.co/meet/\[輸入暱稱\]](https://g.co/meet/[輸入暱稱])
- 前往 meet.google.com 或是 Google Meet 行動應用程式，並在「加入或發起會議」欄位中輸入暱稱

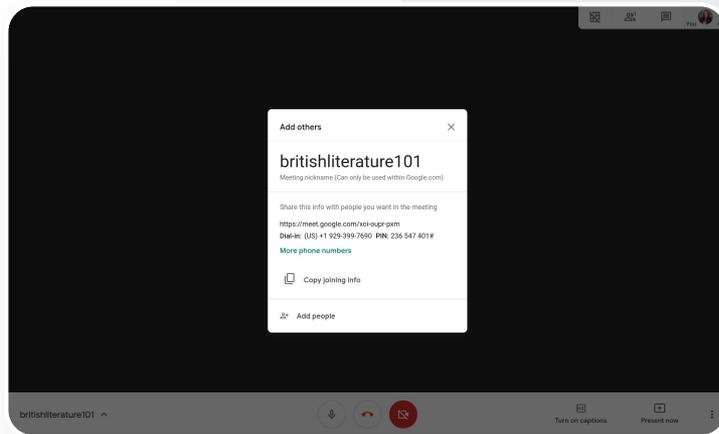
運作方式

老師發起已設定暱稱的會議時，系統會建立一個 10 位數的會議代碼，並且暫時將該代碼與暱稱建立關聯。

在最後一位參與者離開會議或是老師結束會議後，臨時會議代碼就會過期，暱稱與會議代碼間建立的關聯也會失效。

如果學生尚未取得建立會議的權限，就無法使用暱稱或會議代碼。

老師可以重複使用暱稱來建立新的臨時會議代碼，這時學生就可以使用暱稱重新加入會議。



[說明中心相關文件](#)

[與教育相關的 Meet 安全性與隱私權資訊](#)
[發起 Google Meet 視訊會議](#)

錄製課程

Teaching and Learning Upgrade 和 Education Plus 的使用者可以錄製會議，並透過系統自動將會議無限期儲存在雲端硬碟中。

這麼一來，使用者就能輕鬆封存和分享課程、研討會和實作討論會。

- ✓ 如果貴機構的老師使用 Classroom，他們可以透過 Google Meet 整合功能為每個課程分別建立專屬的連結，而這個連結會顯示在 Classroom 的訊息串和課堂作業頁面上。
- ✓ 這類連結形同每一門課程的專屬會議空間，可讓老師和學生輕鬆加入會議。
- ✓ 使用這項整合功能輕鬆錄製課程

[🔗 說明中心相關文件](#)

[為遠距教學設定 Google Meet](#)



我們學校提供大型線上課程，而我們需要為遠距教學和無法出席的學生錄製這些課程。”

[逐步操作說明](#)

錄製教職員會議

有了 Teaching and Learning Upgrade 和 Education Plus, 使用者就能視需求將視訊會議的錄製內容自動儲存至雲端硬碟。這麼一來, 使用者就能輕鬆封存和分享會議、專業發展課程及董事會會議。

- ✓ 建議 IT 管理員僅針對教職員啟用錄製功能
- ✓ 您可以分別為教職員和學生新增機構單位, 然後套用不同的存取規則
- ✓ 如果貴機構使用了 Classroom, 且已有通過驗證的老師, 就能開放授課老師群組存取這項功能

[說明中心相關文件](#)

[為遠距教學設定 Google Meet](#)



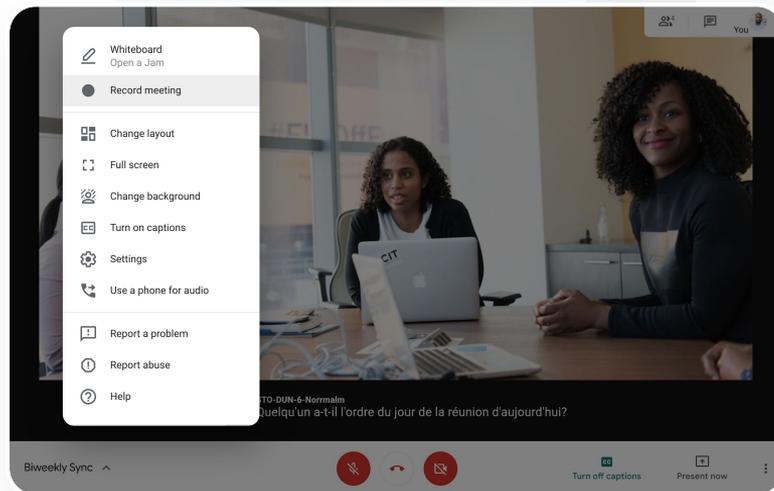
我們會定期舉辦教職員線上會議, 並且需要錄製所有會議。此外, 我們也想錄製專業發展課程及董事會會議。”

[逐步操作說明](#)

操作說明：錄製

如何錄製會議

- 在行事曆中開啟會議並選取「使用 Google Meet 加入會議」
- 在會議確認頁面中，點選右下角的三個垂直圓點來開啟選項選單
- 點選「錄製會議」；螢幕右下角會顯示紅點，表示系統正在錄製會議
- 該會議的影片檔案會自動儲存到您的雲端硬碟中



[說明中心相關文件](#)

[為遠距教學設定 Google Meet](#)

錯過的課程

所有 Teaching and Learning Upgrade 和 Education Plus 的使用者都能存取校內網域的雲端硬碟儲存空間，而視訊會議的錄製內容會自動儲存至會議發起人的雲端硬碟中。如要重播錄製的會議，請向發起人取得錄製內容的連結，或是透過日曆活動存取會議。

- ✓ 錄製內容會儲存在會議發起人的雲端硬碟中
- ✓ 會議主辦人所屬機構單位中的會議參與者也會自動獲得錄製內容的存取權
- ✓ 如果會議發起人改由其他人擔任，系統會將錄製內容的連結傳送給活動的原始建立者

[🔗 說明中心相關文件](#)

[錄製視訊會議內容](#)



我想透過錄製內容觀看
錯過的課程。”

[逐步操作說明](#)

操作說明：觀看及分享錄製內容

如何分享錄製內容

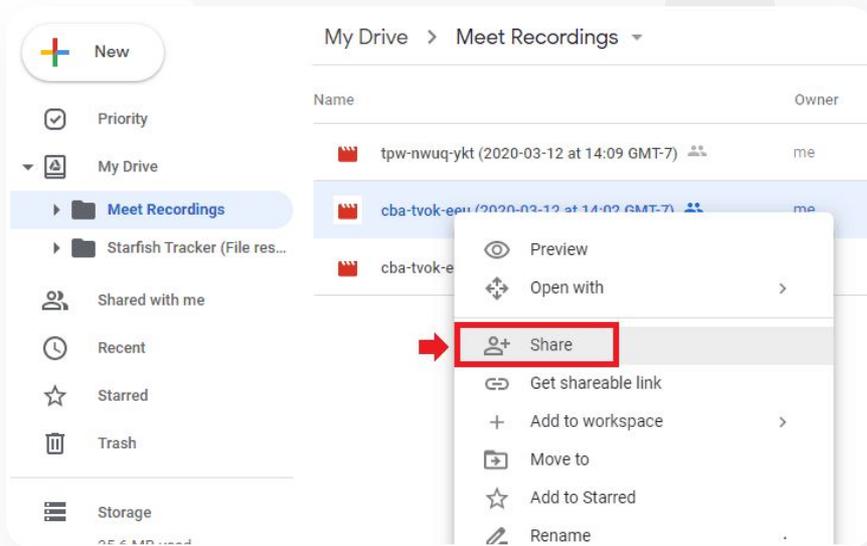
- 選取所需檔案
 - 按一下「分享」圖示
 - 新增核准的檢視者
- 或
- 選取「連結」圖示
 - 在電子郵件或即時通訊訊息中貼上連結

如何下載錄製內容

- 選取所需檔案
- 依序點選「更多」圖示 > 「下載」
- 在下載的檔案上按兩下即可播放

如何播放雲端硬碟中的錄製內容

- 在雲端硬碟中按兩下錄製內容即可播放；在檔案可供線上觀看前，系統會顯示「仍在處理中」
- 如要將錄製內容新增至「我的雲端硬碟」，請選取檔案並按一下「新增至我的雲端硬碟」圖示。



[說明中心相關文件](#)

[錄製視訊會議內容](#)

直播會議

使用 Teaching and Learning Upgrade 進行直播，最多可讓網域內 1 萬人同步觀看；Education Plus 最多則可讓網域內 10 萬人觀看。參與者可以點選發起人在電子郵件中提供的直播連結，或是透過日曆邀請加入會議。請與 IT 管理員合作，確認您有權限加入直播。

- ✓ 建議 IT 管理員僅針對教職員啟用直播功能
- ✓ 如果是大型活動，相較讓使用者加入互動式視訊會議，使用直播能讓使用者獲得更好的體驗
- ✓ 如果使用者錯過直播，可以在會議結束後存取重播

 [說明中心相關文件](#)

[為遠距教學設定 Google Meet](#)



我們需要直播教職員會議，以便供
相關人員和家長觀看。”

[逐步操作說明](#)

直播學校活動

透過直播向學校社群播送學校活動。只要選取發起人透過電子郵件或日曆活動傳送的直播連結即可加入。請與 IT 管理員合作，確認您有權限加入直播。否則請在會議結束後存取[重播](#)。



我們喜歡直播體育賽事和重要活動，像是畢業典禮和返校遊行，讓不能親自到場的人也能參與。”

- ✓ 您可透過 Google Meet 的直播功能與全校社群交流，例如直播畢業典禮、運動賽事或家長會
- ✓ 使用 Teaching and Learning Upgrade 進行直播，最多可讓網域內 1 萬名觀眾同步觀看；Education Plus 則可供最多 10 萬名觀眾觀看

 [說明中心相關文件](#)

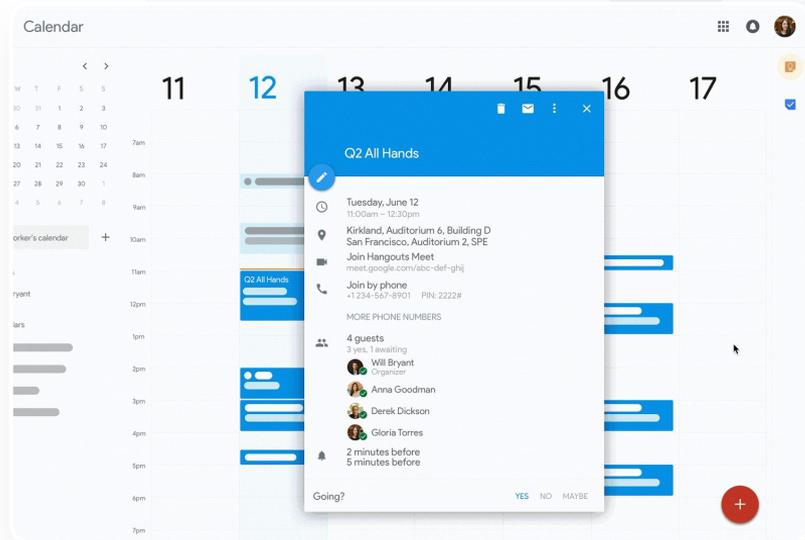
[為遠距教學設定 Google Meet](#)

[逐步操作說明](#)

操作說明：直播

如何授予直播權限

- 開啟 Google 日曆
- 選取「加號建立」>「更多選項」
- 新增活動詳細資料，例如日期、時間和說明
- 最多可新增 250 位在視訊會議中具備完整存取權限的邀請對象，這表示受邀者能看到彼此的影像，聽到彼此的發言，也能分享自己的螢幕畫面；您也可以新增其他機構的邀請對象
- 點選「新增會議」>「Meet」
- 在「加入 Meet 通話」旁選取向下箭頭，接著選取「新增直播」
- 如要在網域內邀請貴機構使用的付費版本允許的上限人數，請點選複製直播網址，並透過電子郵件或即時通訊訊息分享連結
- 選取儲存
- 系統不會自動開始直播；在會議開始後，選取更多 > 開始直播



[說明中心相關文件](#)

[為遠距教學設定 Google Meet](#)

注意：只有貴機構中的邀請對象才能觀看直播 內容

提出問題

使用 Google Meet 的問與答功能維持學生參與度，並增加課程中的互動。教育工作者還可以在虛擬課程結束時，取得所有問與答的詳細報告。

- ✓ 主持人可視需求盡情提問，不受次數限制。還可以過濾問題、將問題加以分類、標示為已回答，甚至是隱藏或優先顯示問題。
- ✓ 在啟用問與答功能的會議結束後，系統會透過電子郵件自動傳送問題報告給主持人。

[🔗 說明中心相關文件](#)

[在 Google Meet 中向參與者提問](#)



我需要快速張貼問題、測量學生知識，並在課程中和學生互動以維持他們的參與度。”

[逐步操作說明](#)

操作說明：問與答

提出問題：

- 在會議中，依序選取右上角的「活動」圖示 > 「問題」(如要開啟問與答功能，請選取「開啟問與答」)
- 如要提問，請在右下角點選「提出問題」
- 輸入問題 > 選取「張貼」

查看問題報告：

- 會議結束後，主持人會收到含有問題報告的電子郵件
- 開啟電子郵件 > 按一下報告中的附件



[🔗 說明中心相關文件](#)

[在 Google Meet 中向參與者提問](#)

收集意見

預先排定或發起虛擬會議的使用者可以為與會者建立意見調查。這項功能可以協助主持人快速收集所有與會學生或參與者的資訊。

- ✔ 主持人可以預先儲存意見調查，等到會議開始進行後再張貼。
意見調查會儲存在虛擬會議中的意見調查專區，方便主持人管理。
- ✔ 會議結束後，系統會透過電子郵件自動將意見調查結果傳送給主持人。

[🔗 說明中心相關文件](#)

[在 Google Meet 中進行意見調查](#)



“我需要在主導課程或教職員會議時，快速收集學生和其他教育工作者的想法。”

[逐步操作說明](#)

操作說明：進行意見調查

建立意見調查：

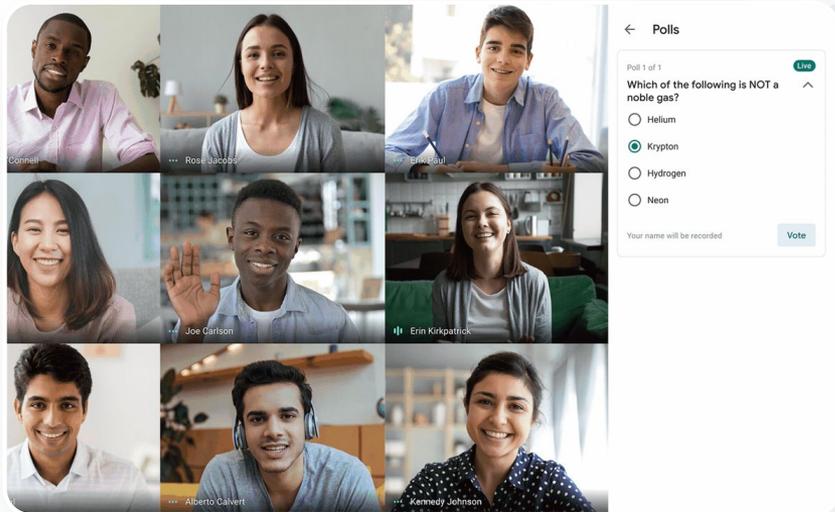
- 在會議中，依序選取右上角的「活動」圖示 > 「意見調查」
- 選取「發起意見調查」
- 輸入問題
- 選取「發布」或「儲存」

管理意見調查：

- 在會議中，依序選取右上角的「活動」圖示 > 「意見調查」
- 如要讓參與者即時查看意見調查結果，請在向所有人顯示結果旁邊的按鈕上選取切換為開啟
- 如要關閉意見調查並禁止回覆，請按一下「結束意見調查」
- 如要永久刪除某個意見調查，請選取「刪除」圖示

查看意見調查報告：

- 會議結束後，主持人會收到含有報告的電子郵件
- 開啟電子郵件 > 選取報告中的附件



[🔗 說明中心相關文件](#)

[在 Google Meet 中進行意見調查](#)

學生小組

教育工作者可以使用分組討論室，將虛擬會議中的學生分成多個小組。主持人必須使用電腦，才能在視訊通話期間建立分組討論室。目前系統無法直播或錄製分組討論室的會議過程。

- ✓ 每場虛擬會議最多可以建立 100 間分組討論室
- ✓ 老師可以輕鬆在分組討論室間移動，為有需要的小組提供協助
- ✓ 管理員可以確保只有教職員能建立分組討論室

 [說明中心相關文件](#)

[使用 Google Meet 的分組討論室功能](#)



我們現在全面採取遠距學習，因此需要能模擬實體授課的方法，以便輕鬆將孩子分組、在會議室中移動以便旁聽和加入討論，並快速重新召集各小組。”

[逐步操作說明](#)

操作說明：建立分組討論室

如何建立分組討論室

- 發起視訊通話。
- 選取右上方的「活動」圖示 > 「分組討論室」。
- 在分組討論室面板中，選擇需要的分組討論室數量。
- 系統會自動將學生分配到各個討論室，但主持人能視情況手動將學生移到不同的討論室。
- 按一下右下方的「開啟」分組討論室。

在不同的分組討論室中回答問題

- 參與者尋求協助時，主持人的螢幕下方會顯示通知。如要加入參與者的分組聊天室，請選取加入」。



[說明中心相關文件](#)

[使用 Google Meet 的分組討論室功能](#)

追蹤出席狀況

出席狀況追蹤功能可針對有 5 位以上參與者的會議，自動產生出席狀況報告。報告會顯示加入通話的參與者、他們的電子郵件，以及待在虛擬課程中的時間。

- ✔ 您可以使用直播報告來追蹤直播活動期間的出席狀況
- ✔ 主持人可以在會議或日曆活動中選擇是否要開啟出席狀況追蹤功能和直播報告

 [說明中心相關文件](#)

[追蹤 Google Meet 會議的出席情況](#)



我們難以追蹤有誰參與了線上課程。我需要方便的回報機制，讓我能掌握整個網域內的課程出席狀況。”

[逐步操作說明](#)

操作說明：出席狀況報告

在會議中：

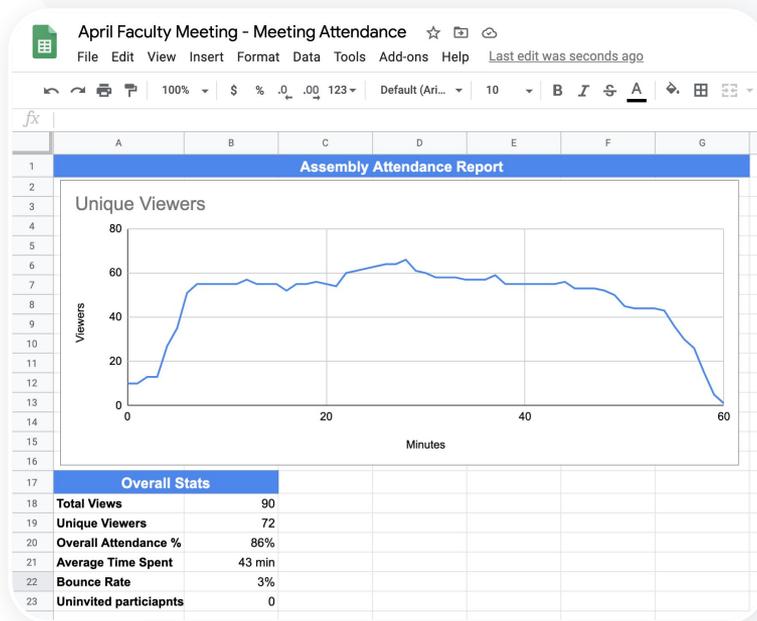
- 發起視訊通話
- 選取底部的「選單」圖示
- 依序選取「設定」圖示 > 「主辦人控制項」
- 開啟或關閉出席狀況追蹤

透過日曆：

- 在日曆活動中啟用 Google Meet 會議通訊
- 選取畫面右側的「設定」圖示
- 勾選「出席狀況追蹤」旁的方塊 > 按一下「儲存」

取得出席狀況報告：

- 會議結束後，主持人會收到含有報告的電子郵件
- 開啟電子郵件 > 選取報告中的附件



[說明中心相關文件](#)

[追蹤 Google Meet 會議的出席情況](#)

謝謝您