個人電腦資訊安全自我檢查表操作說明

(國立嘉義高商 v20241004)

臨時修正項目：

20250225 修正 DNS 設定第 3-5 頁

20250602 修正 Windows 版本查詢第 11 頁

參閱本文件之前，請先閱讀本頁說明

●文件編排方式：每個主題先以文字說明，相關圖片在每個主題後方，請自行對照。

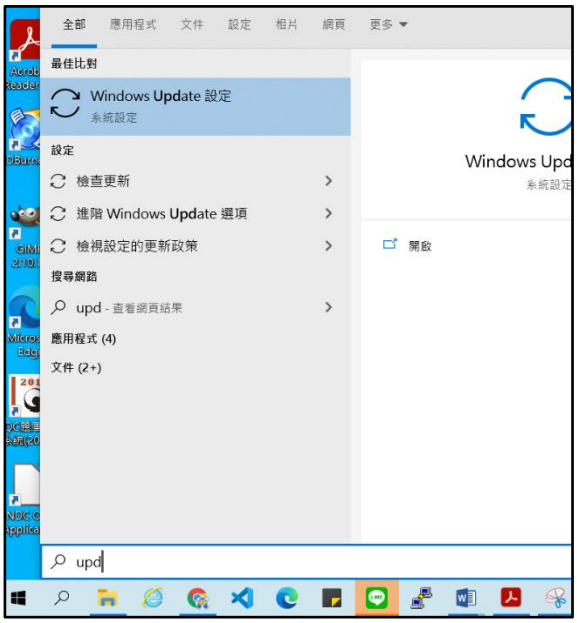
●操作前說明：後面的操作中，常會用到底下兩種方式，請先了解用法

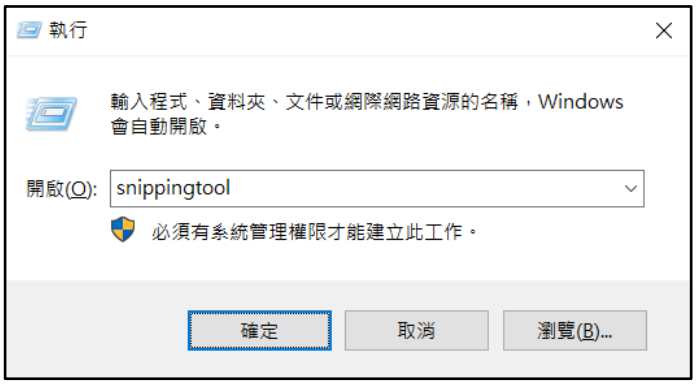
一、在 Windows10 中利用**搜尋**方式比較容易找到要執行的程式，操作如下：

按**鍵盤左下角的 鍵**，或滑鼠點選工作列**左側的放大鏡**，然後**直接輸入關鍵字**，如 cmd、本機安全性原則…通常就會跳出我們要的程式

二、如果你知道程式的執行檔名，可以利用執行框**直接輸入指令執行**，操作如下：

按下**鍵盤的 +R**，會跳出**執行視窗**，**直接輸入執行檔**名稱，如 cmd、snippingtool、winword、secpol.msc…其中 cmd 是命令提示字元，snippingtool 是剪取工具，winword 是 Word，而 secpol.msc 是本機安全性原則，而且之前輸入過的指令會記錄下來，可以重複使用，非常推薦大家日常使用。





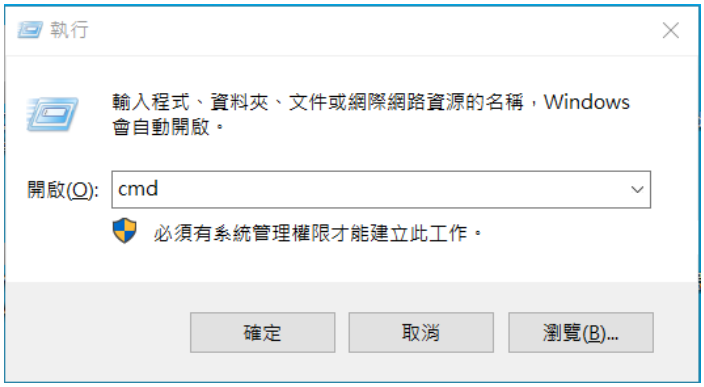
注意：本操作中所提供的方法並非唯一，通常有更多不同的方式，可依自己需求進行操作及檢查。

○、個人電腦網路設定資訊查詢

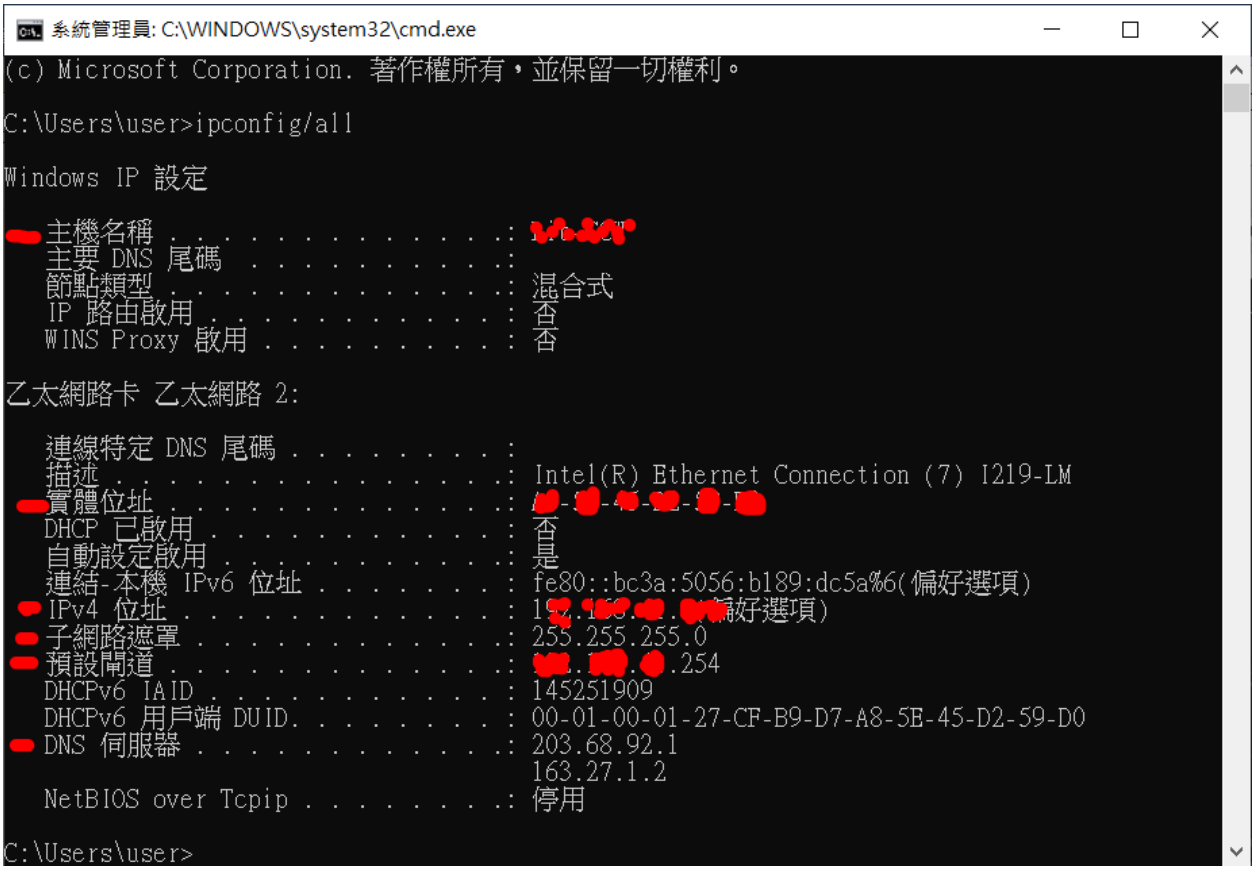
1. 開啟命令提示字元：利用前頁所說的操作方式，搜尋或直接執行 **cmd** 。

2. 指令：**ipconfig /all** ，確認基本資訊，最好將底下的資訊記錄下來。

   A. **主機名稱**：Windows 中設定的電腦名稱。
   B. **實體位址**：網卡的 Mac Address，6 組十六進位數字(Hex)，以 **-** 或 **：** 隔開。
   C. **IPv4 位址**：4 個十進位數字，以 **.** 隔開 (如果有很多組，找 **192.168.**開頭的)。
   D. 檢查子網路遮罩和預設閘道：需配合 IPv4 位址，設定錯誤則無法正常上網。
   E. DNS 伺服器：依「校內資安訊息/DNS」說明設定，DNS 建議設定兩組，一組設定學術網路(**140.111.233.5** 或 **163.28.6.1** 擇一)，另一組設其他單位(中華電信 **168.95.1.1**、~~Google **8.8.8.8** 擇一~~)，兩組互為備援，若不是設定為這兩組，請修改設定。



小常識：因為檔案要上網，所以關鍵資料要碼賽克(如下圖)，避免洩漏重要資訊…



3. 變更網域名稱伺服器 DNS (檢查

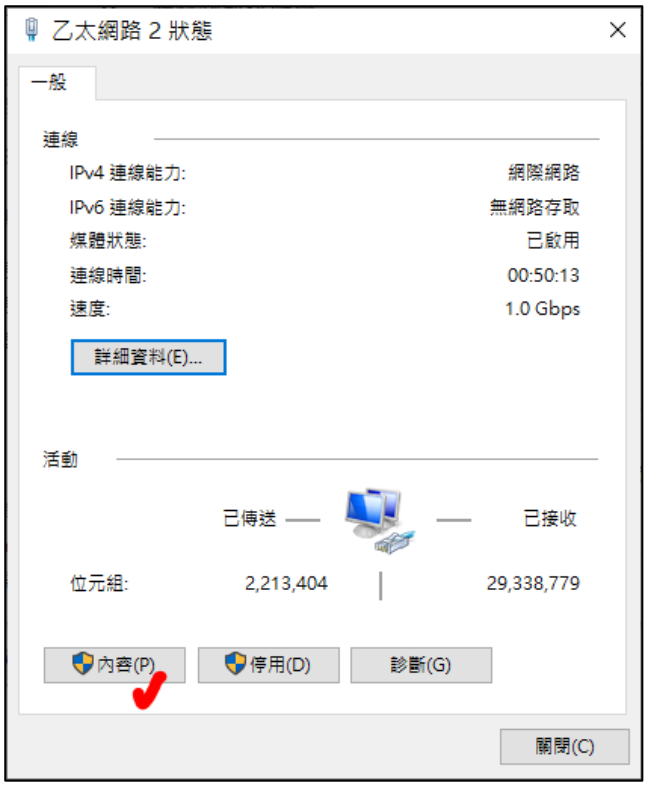
A. 網路狀態：左下角按「**滑鼠右鍵**」，選「網路連線」，或搜尋「網路狀態」

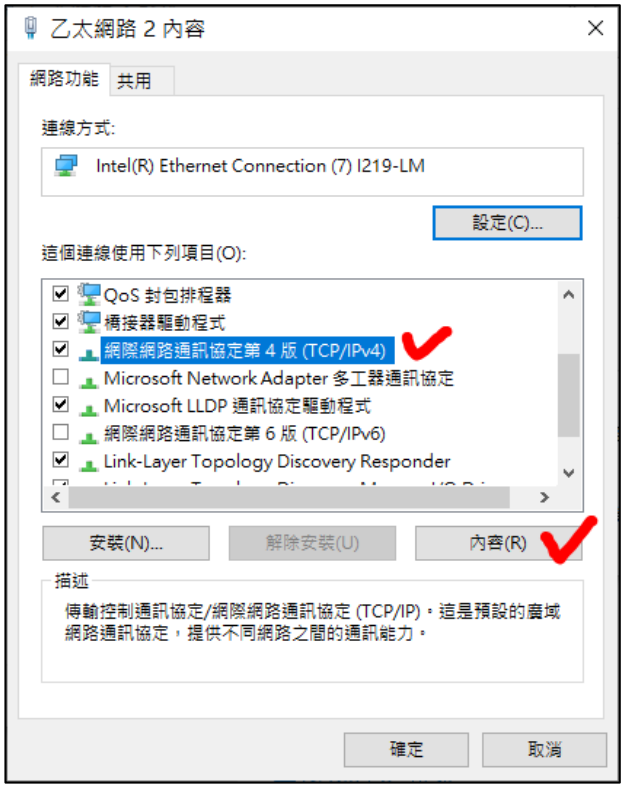
B. 網路共用中心：出現「網路狀態」的畫面，點選「**網路共用中心**」，

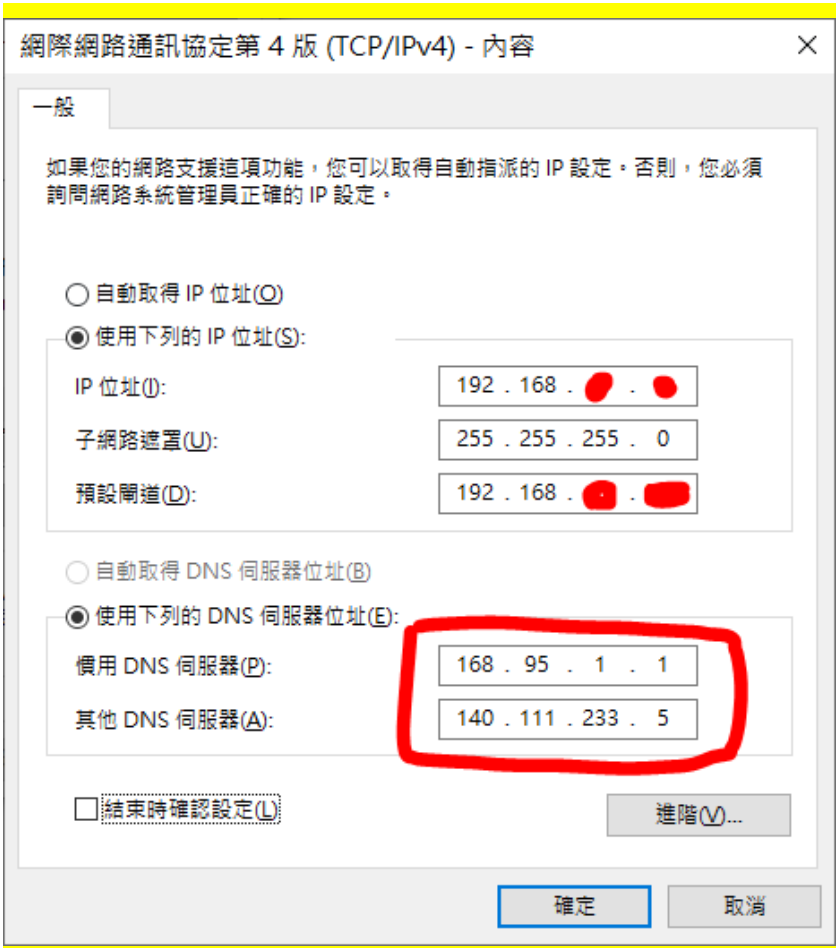
C. 點選右側連線的「**乙太網路 2**」(每台電腦的網路名可能會不一樣)。跳出視窗後，再點選「內容」按鈕。

D. 找到「**網際網路通訊協定第 4 版(TCP/IPv4)**」，點選下方的「**內容**」按鈕。

E. 檢查或更改 DNS，詳見學校首頁/左側選單/校內資安訊息，兩組 DNS 均要設定。
一組設定教育部「**140.111.233.5** 或 **163.28.6.1**」擇一
另一組設定外部單位 ~~Google **8.8.8.8** 或~~中華電信 **168.95.1.1** ~~擇一~~。

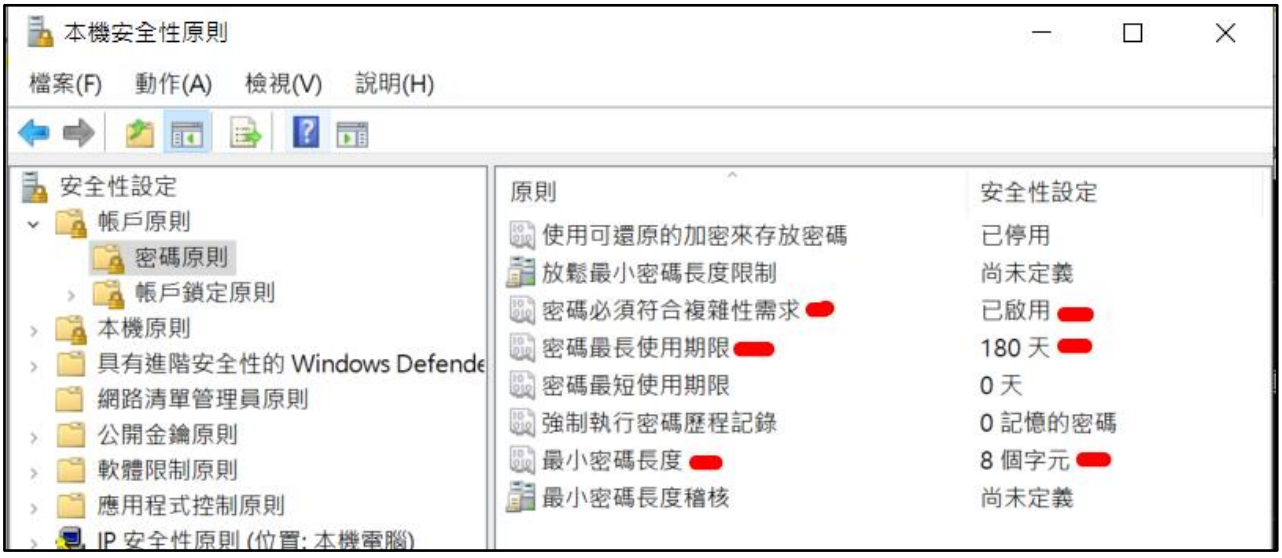

乙太網路 2 狀態
一般
連線
IPv4 連線能力: 網際網路
IPv6 連線能力: 無網路存取
媒體狀態: 已啟用
連線時間: 00:50:13
速度: 1.0 Gbps
詳細資料(E)...
活動
已傳送
已接收
位元組: 2,213,404 29,338,779
內容(P)
停用(D)
診斷(G)
關閉(C)

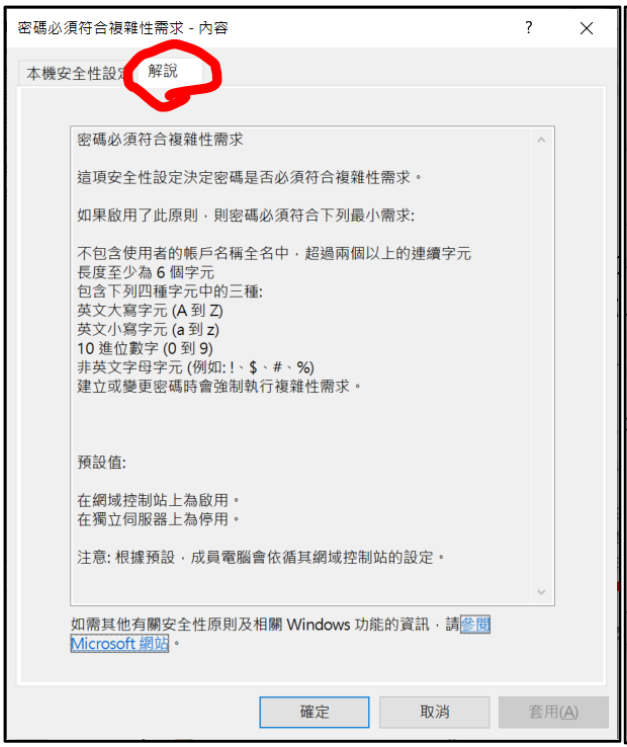

乙太網路 2 內容
網路功能
共用
連線方式:
Intel(R) Ethernet Connection (7) I219-LM
設定(C)...
這個連線使用下列項目(O):
QoS 封包排程器
橋接器驅動程式
網際網路通訊協定第 4 版 (TCP/IPv4)
Microsoft Network Adapter 多工器通訊協定
Microsoft LLDP 通訊協定驅動程式
網際網路通訊協定第 6 版 (TCP/IPv6)
Link-Layer Topology Discovery Responder
安裝(N)...
解除安裝(U)
內容(R)
描述
傳輸控制通訊協定/網際網路通訊協定 (TCP/IP)。這是預設的廣域網路通訊協定，提供不同網路之間的通訊能力。
確定
取消

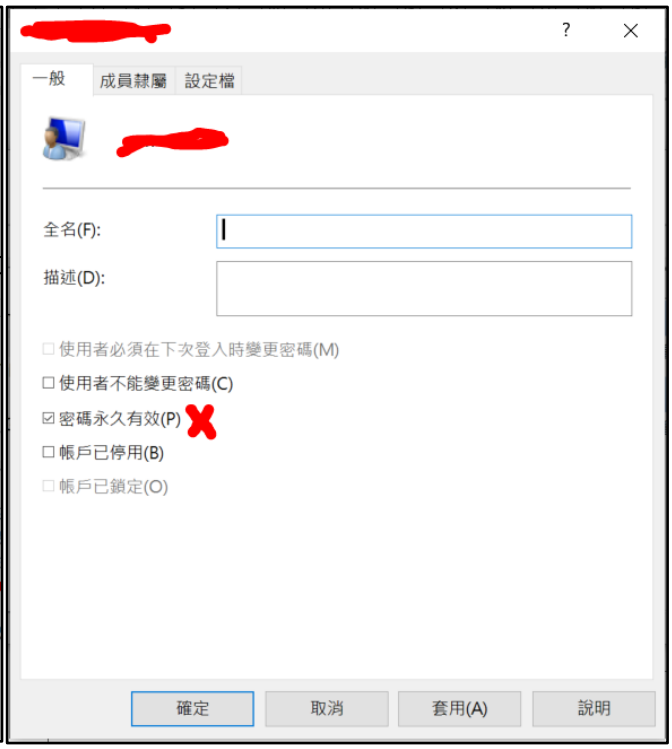

網際網路通訊協定第 4 版 (TCP/IPv4) - 內容
一般
如果您的網路支援這項功能，您可以取得自動指派的 IP 設定。否則，您必須詢問網路系統管理員正確的 IP 設定。
自動取得 IP 位址(O)
使用下列的 IP 位址(S):
IP 位址(I): 192 . 168 . [redacted]
子網路遮罩(U): 255 . 255 . 255 . 0
預設閘道(D): 192 . 168 . [redacted]
自動取得 DNS 伺服器位址(B)
使用下列的 DNS 伺服器位址(E):
慣用 DNS 伺服器(P): 168 . 95 . 1 . 1
其他 DNS 伺服器(A): 140 . 111 . 233 . 5
結束時確認設定(L)
進階(V)...
確定
取消

一、密碼安全性設定及密碼設定

1. 應設定**(1)密碼原則　(2)取消密碼永久有效的設定。**
2. 密碼原則設定如下：
   A. 本機安全性原則：搜尋「本機安全性原則」或直接執行 **secpol.msc**
   B. 要設定**(1)複雜性需求 (2)最長使用期限 180 以下 (3)最小密碼長度 8 以上**。滑鼠點兩下就可以修改，每一項設定都可以看一下【解說】，比如下圖，可以了解 Windows 對所謂【複雜性密碼】的規定為何？
3. 取消密碼永久有效的設定：
   A. 本機使用者和群組：搜尋「電腦管理」或直接執行 **lusrmgr.msc**
   B. 選擇「本機使用者和群組」下的「使用者」，在視窗中間找到自己的登入帳號(通常是 USER)，順便檢查一下不應該有陌名其妙的帳號…(確認 Guest 帳戶是停用)
   C. 在自己的帳號點兩下滑鼠，**取消密碼永久有效** (不要勾選)。
   D. 可以順便變更一下密碼，以符合要求。在帳號按滑鼠右鍵可以變更密碼。
4. 查詢上次變更密碼日期：
   A. 「cmd」開啟命令提示字元，指令「net user 你的帳號」




密碼必須符合複雜性需求 - 內容
本機安全性設定
解說
密碼必須符合複雜性需求
這項安全性設定決定密碼是否必須符合複雜性需求。
如果啟用了此原則，則密碼必須符合下列最小需求:
不包含使用者的帳戶名稱全名中，超過兩個以上的連續字元
長度至少為 6 個字元
包含下列四種字元中的三種:
英文大寫字元 (A 到 Z)
英文小寫字元 (a 到 z)
10 進位數字 (0 到 9)
非英文字母字元 (例如: !、$、#、%)
建立或變更密碼時會強制執行複雜性需求。
預設值:
在網域控制站上為啟用。
在獨立伺服器上為停用。
注意: 根據預設，成員電腦會依循其網域控制站的設定。
如需其他有關安全性原則及相關 Windows 功能的資訊，請參閱 Microsoft 網站。
確定
取消
套用(A)


一般
成員隸屬
設定檔
全名(F):
描述(D):
使用者必須在下次登入時變更密碼(M)
使用者不能變更密碼(C)
密碼永久有效(P)
帳戶已停用(B)
帳戶已鎖定(O)
確定
取消
套用(A)
說明


系統工具
工作排程器
事件檢視器
共用資料夾
本機使用者和群組
使用者
群組
效能
裝置管理員
存放裝置
磁碟管理
Administrator
管理電腦/網域的內建帳戶
DefaultAccount
Guest
WDAGUtilityAccount
設定密碼(S)...
所有工作(K)
刪除(D)
重新命名(M)
內容(R)
說明(H)
使用者
其他動作
其他動作


系統管理員: 命令提示字元
(c) Microsoft Corporation. 著作權所有，並保留一切權利。
C:\Users\user>net user
指令：net user 你的帳號
帳號：登入畫面會看到的
使用者名稱
註解
使用者的註解
國家/區域碼 000 (系統預設值)
帳戶使用中 Yes
帳戶到期 從不
上次設定密碼 2024/10/4 下午 02:47:35
密碼到期 2025/4/2 下午 02:47:35
可變更密碼 2024/10/4 下午 02:47:35
請輸入密碼 No
使用者可以變更密碼 Yes
容許的工作站 全部
登入指令檔
使用者設定檔
主目錄
上次登入時間 2024/10/4 下午 02:58:00
可容許的登入時數 全部
本機群組會員
全域群組會員 *None
命令已經成功完成。


帳號
文件
圖片
設定
電源

二、螢幕保護密碼設定

1. 設置螢幕保護程式可以減少螢幕損耗、省電，設置密碼可以避免別人私自使用您的電腦，設置時間太長缺乏保護效果，設置時間太短可能會影響自身工作。
2. 密碼原則設定如下：

   A. 螢幕保護裝置設定：搜尋「**螢幕保護**」或 **screensaver**。

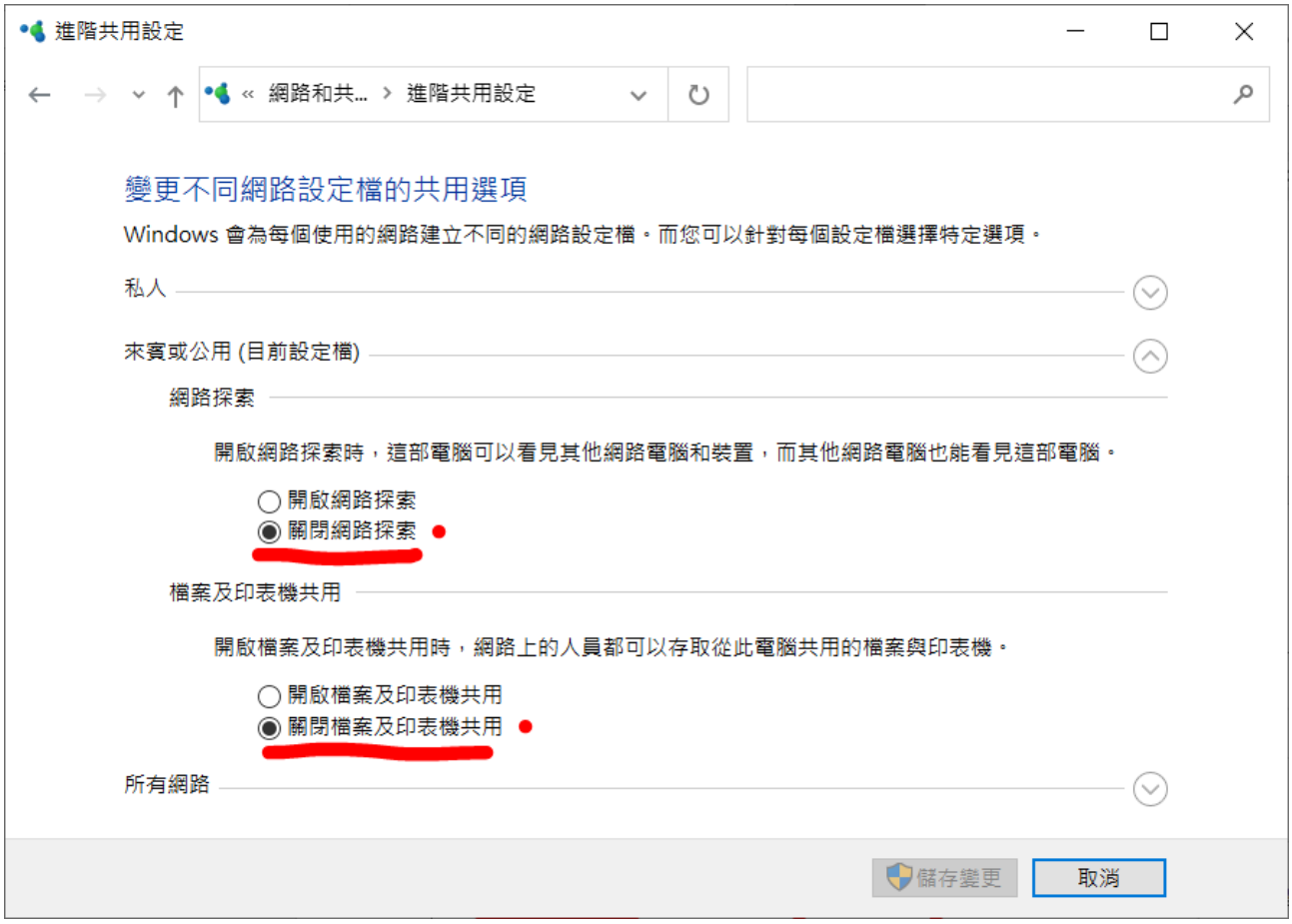
   B. 或桌面上按右鍵「**個人化/左側，鎖定畫面/螢幕保護程式設定**」。

   C. **【繼續執行後，顯示登入畫面】一定要打勾**，營幕保護裝置建議設置為「空白」最具保護效果，等候時間最多 **10** 分鐘，建議不要超過 3 分鐘。

三、關閉資源分享

1. 應設定**(1)網路和共用中心設為公用網路　(2)檢查共用資料夾設定**。
2. 設定為公用網路，關閉網路探索、檔案及印表機共用。
   A. 網路和共用中心：搜尋「網路狀態」或在工作列開始鈕 上按右鍵，選**網路連線**
   B. 網路狀態視窗中找到網路和共用中心，並選擇左側的**變更進階共用設定**。
   C. **公用網路**：預設為**關閉網路探索**、**關閉檔案及印表機共用**(多數人用不到)。
   D. 注意：上述設定可能會影響**印表機掃描程式**或**天方系統**，請向廠商確認相關情形，若有此狀況，請註記在檢查表中。
3. 檢查共用資料夾
   A. 共用資料夾：搜尋「電腦管理」或直接執行 **fsmgmt.msc**
   B. 點選「共用」，視窗中間會列出目前設定為共用的資料夾，除了幾個預設的外(參考下圖)，如果有其他不明原因的共用資料夾，請按滑鼠右鍵停止共用。
   C. 注意：某些**【舊】**系統，會使用共用資料夾連線系統主機，請務必確認後再使用。

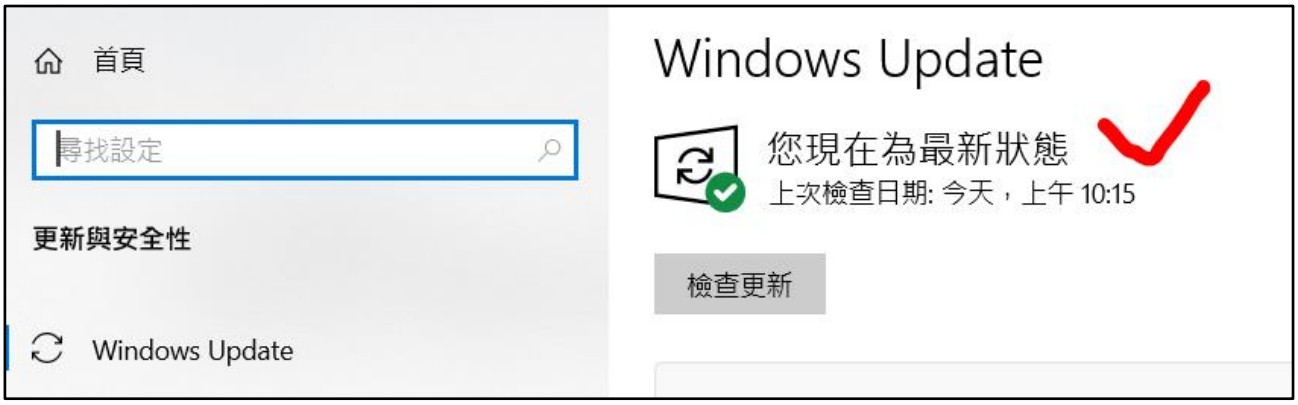

網路和共用中心
所有控... › 網路和共用中心
檢視您基本的網路資訊並設定連線
控制台首頁
變更介面卡設定
變更進階共用設定
媒體串流選項
檢視作用中的網路
網路 3
公用網路
存取類型: 網際網路
連線: 乙太網路 2
變更網路設定
設定新的連線或網路


進階共用設定
網路和共... › 進階共用設定
變更不同網路設定檔的共用選項
Windows 會為每個使用的網路建立不同的網路設定檔。而您可以針對每個設定檔選擇特定選項。
私人
來賓或公用 (目前設定檔)
網路探索
開啟網路探索時，這部電腦可以看見其他網路電腦和裝置，而其他網路電腦也能看見這部電腦。
開啟網路探索
關閉網路探索
檔案及印表機共用
開啟檔案及印表機共用時，網路上的人員都可以存取從此電腦共用的檔案與印表機。
開啟檔案及印表機共用
關閉檔案及印表機共用
所有網路
儲存變更
取消


共用資料夾
檔案(F) 動作(A) 檢視(V) 說明(H)
共用資料夾 (本機)
共用
工作階段
開啟檔案
共用名稱 資料夾路徑 類型 # 用戶端連線 描述
ADMIN$ C:\WINDOWS Windows 0 遠端管理
C$ C:\ Windows 0 預設共用
D$ D:\ Windows 0 預設共用
IPC$ Windows 0 遠端 IPC

四、作業系統自動更新

1. 作業系統更新：搜尋「**update**」，點選「Windows Update 設定」或「檢查更新」。
2. 請確保 Windows 為更新至最新狀態，並請勿任意設定為暫停更新。



3. 版本檢查：搜尋或直接執行 **winver.exe**

4.

五、檢視電腦中已安裝的程式

1. 個人電腦安全檢查表中第 5、6、7、8 項均需檢查已安裝軟體。
2. 應執行**(1)檢查來路不明或未授權軟體 (2)檢查重要軟體版本並更新**，如 Chrome、Edge、Java、Adobe Reader、7-Zip、ODF 工具… **(3)移除不當軟體或危害網路之軟體**，如 P2P、挖礦軟體、Flash Player、Win-Rar **(4)勿常駐遠端連線桌面軟體**。
3. 程式和功能：搜尋「**應用程式與功能**」或開啟控制臺，點選「**程式和功能**」或直接 win+R 執行 **appwiz.cpl (建議)**，(方便檢查版本、安裝/更新日期)
4. 平時請留意所安裝的程式，並了解其用途(可上網查軟體名稱)，若有不熟悉的軟體，或突然出現的軟體，可能是被挾帶安裝或惡意程式，請**儘量移除不需要使用的軟體**
   A. 程式清單中除了一般應用軟體外，可能還會出現一些微軟函式庫的套件(請參考圖解)，注意發行者是 Microsoft Corporation 這是正常情況。
   B. 其他你未知的軟體，可上網查詢，了解軟體作用及是否有害。
5. 請**留意軟體的版權**，除了使用正版軟體外，有些免費軟體僅授權【家用】，學校電腦並不屬於【家用】，所以不在免費使用範圍。(比較常見的是免費防毒軟體…) 。
6. **瀏覽器設定自動更新**：請參閱「九、完成瀏覽器的安全設定」。
7. **Java 檢測：**
   A. 說明：在電腦或瀏覽器中執行 Java 程式時，需安裝 Java 執行。目前新版的 Chrome、Edge 瀏覽器已不支援在瀏覽器中執行 Java 程式(或 Java Applet)
   B. 檢查電腦是否安裝 Java，並確認其版本。
   參考官網建議版本 https://www.java.com/zh-TW/download/
   C. 如果已安裝 Java 請確認更新 Java 至最新版本
   https://www.java.com/zh-TW/download/help/version_manual.html
   D. **建議：如非必要，請移除 Java**。
   https://www.java.com/zh-TW/download/help/uninstaller_toolfaq.html
8. **Adobe Flash Player 請移除！！**
   A. 說明：早期許多網頁程式及動畫採用 flash 製作，瀏覽器需加裝 flash palyer 播放，但 flash palyer 有非常多的漏洞，不建議繼續使用，目前網頁中大多以 HTML5 替代，且大多數瀏覽器均已不支援 flash player。
   B. 檢查電腦是否安裝 flash player，如果有，**請移除所有 flash player 相關軟體**
9. **Adobe Arcobat Reader 檢測**
   A. Adobe Reader 是常見的 PDF 免費瀏覽工具。
   B. 檢查電腦是否安裝 Adobe Reader，並確認其版本，保持更新。
   C. 版本資訊 https://helpx.adobe.com/tw/acrobat/release-note/release-notes-acrobat-reader.html
10. 壓縮軟體：
    A. Windows 10 以後已內建 ZIP 壓縮格式，但仍有許多壓縮格式無法解開，因此通常會多安裝壓縮及解壓縮軟體，早期常用的 WinRAR 是版權軟體，雖然有試用版，但目前被揭露的漏洞風險較多，且軟體更新不夠即時，因此不建議使用，有安裝 WinRAR 的請解除安裝。
    B. 建議安裝使用 7-Zip (https://www.7-zip.org/)，是自由軟體、免費且沒有授權的問題，

目前更新穩定。不過 7-Zip 沒有自動更新機制，使用者應定期檢視並**手動更新**。

11. ODF 應用文件程式：
    A. 軟體名為 MODA ODF Application Tools 為數位發展部所提供，適合公務機關使用的軟體，唯該軟體並沒有自動更新的機制，使用者應定期檢視並**手動更新**。
    B. 使用者也可以使用支援 ODF 的 Libre Office 等工具。

12. P2P 軟體下載軟體

A. 依教育部台電字第 0970077254 號函，學術網路全面禁止使用點對點互連(P2P)軟體下載或提供分享版權軟體及影音檔案。
B. 使用 P2P 點對點下載軟體(BitTorrent)，容易佔用大量網路頻寬，下載及上傳未經授軟體、影片，是病毒、惡意軟體的溫床，可能造成網路變慢、違法、中毒等嚴重後果。
C. 學校嚴禁使用相關軟體，請移除。

13. **遠端桌面連線軟體**(或遠端登入)
    A. 透過遠端桌面軟體可以從外操作電腦，因此開放遠端桌面連線是相常危險的。
    B. 遠端桌面(Remote Desktop Protocol，**RDP**，連接埠 3389)，**使用原則**：
    (1). 遠端桌面使用時機通常為(a)**尋求支援**：因外地的技術支援等原因而開放工程師透過遠端桌面連入協助處理或教學，或(b)**異地工作**：由家裡或其他地方連線回辦公室電腦作業(此種情況最好透過 SSLVPN)，因此使用時機通常為**特定已知對象**。
    (2). 不應該長期開放遠端桌面(常駐)，需要使用時再開放。**(要用再開)**
    (3). 開放遠端桌面之前，應設定防火牆**限定特定來源 IP** 才能連線。
    (4). 尋求遠端支援(教學)時，**當事人應在電腦前了解其操作內容**。
    (5). 異地工作自行開放遠端桌面時，應透過 SSLVPN 連線，並設定安全的連線密碼。
    C. 常見遠端桌面軟體：I
    (1). Windows 內建遠端桌面連線 mstsc.exe、快速助手。
    (2). **Chrome Remote Desktop**、**TeamViewer**、**AweSun**、**AnyDesk**…。
    (3). 遠端桌面連線軟體非常多，請檢查已安裝軟體並查明其用途。
    D. 關閉遠端桌面連線

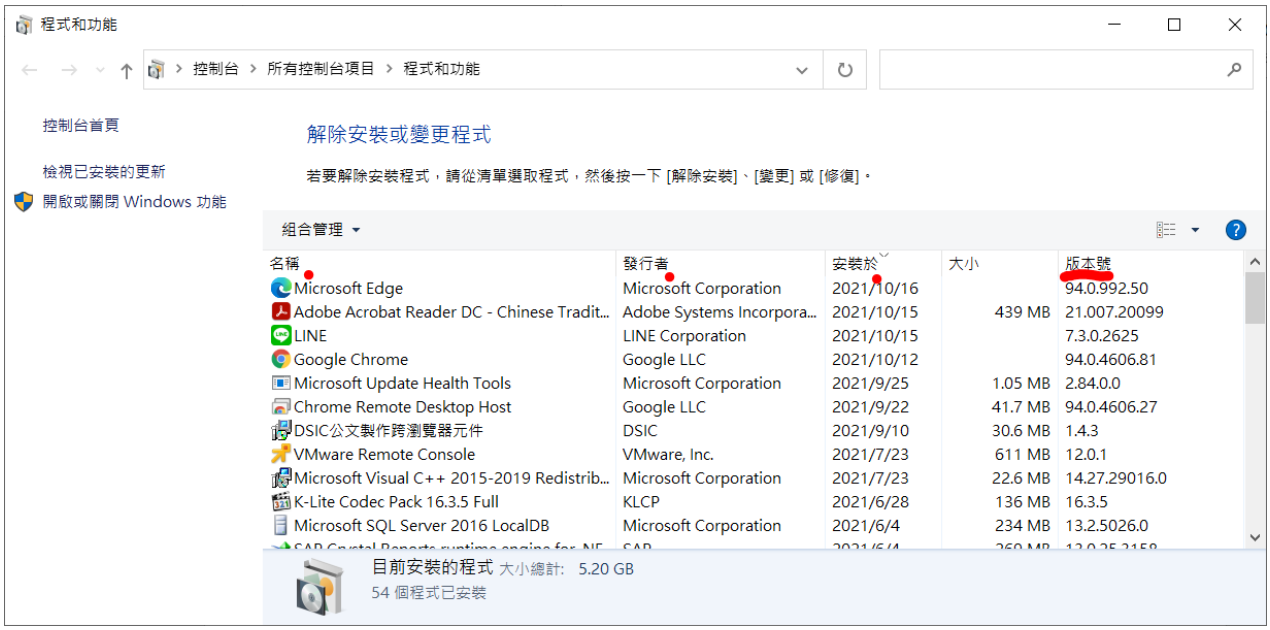
(1). Windows 內建：搜尋「遠端桌面設定」或直接執行 **sysdm.cpl**

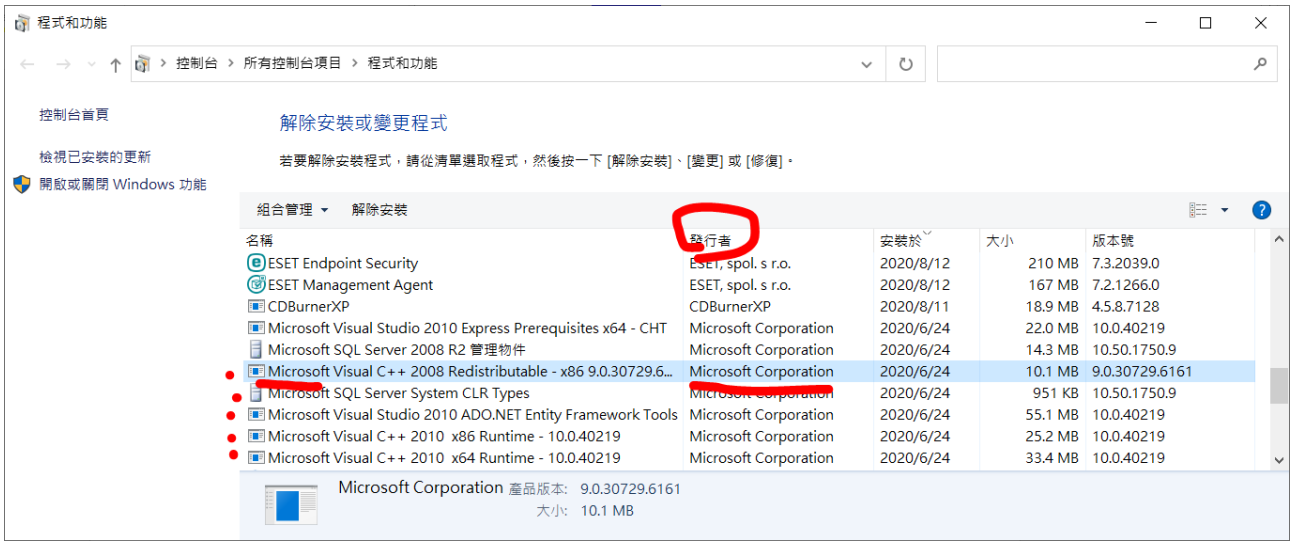
(2). 其他軟體：這類軟體通常分為**常駐(安裝、永久密碼…)**和**啟動程式後接受遠端連線**兩類，**不要直接安裝並常駐使用！**也不要使用固定的連線授權碼，要用時再執行並取得新的授權碼。

注意：後面遠端桌面設定的圖是兩個不同設定方式，擇一即可。

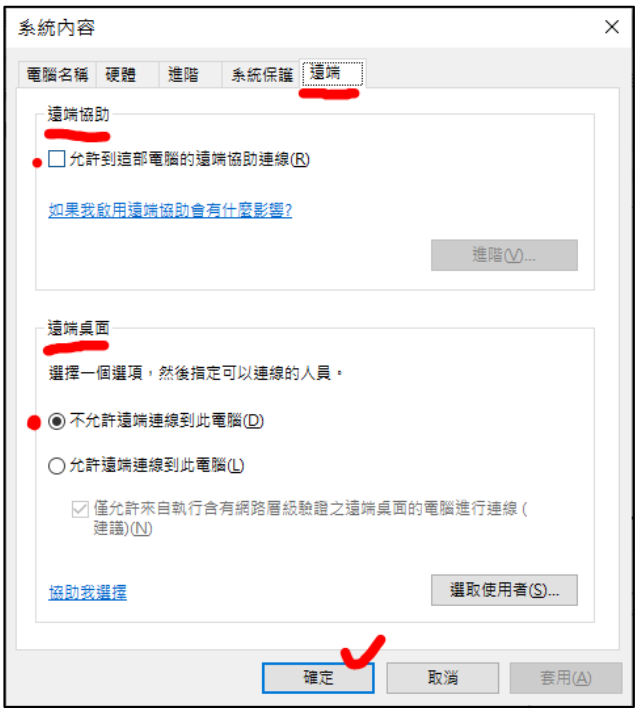
E. 公務上，廠商需遠端連線：

(1). 學校防火牆已阻斷大多數遠端桌面連線，如公務上需要廠商遠端連線操作，請洽圖書館申請開放。
(2). 如前項 D 之(2)條所述，需要時再開啟程式，平時應保持關閉。


程式和功能
控制台 › 所有控制台項目 › 程式和功能
控制台首頁
檢視已安裝的更新
開啟或關閉 Windows 功能
解除安裝或變更程式
若要解除安裝程式，請從清單選取程式，然後按一下 [解除安裝]、[變更] 或 [修復]。
組合管理
名稱 發行者 安裝於 大小 版本號
Microsoft Edge Microsoft Corporation 2021/10/16 94.0.992.50
Adobe Acrobat Reader DC - Chinese Tradit... Adobe Systems Incorpora... 2021/10/15 439 MB 21.007.20099
LINE LINE Corporation 2021/10/15 7.3.0.2625
Google Chrome Google LLC 2021/10/12 94.0.4606.81
Microsoft Update Health Tools Microsoft Corporation 2021/9/25 1.05 MB 2.84.0.0
Chrome Remote Desktop Host Google LLC 2021/9/22 41.7 MB 94.0.4606.27
DSIC公文製作跨瀏覽器元件 DSIC 2021/9/10 30.6 MB 1.4.3
VMware Remote Console VMware, Inc. 2021/7/23 611 MB 12.0.1
Microsoft Visual C++ 2015-2019 Redistrib... Microsoft Corporation 2021/7/23 22.6 MB 14.27.29016.0
K-Lite Codec Pack 16.3.5 Full KLCP 2021/6/28 136 MB 16.3.5
Microsoft SQL Server 2016 LocalDB Microsoft Corporation 2021/6/4 234 MB 13.2.5026.0
目前安裝的程式 大小總計: 5.20 GB
54 個程式已安裝

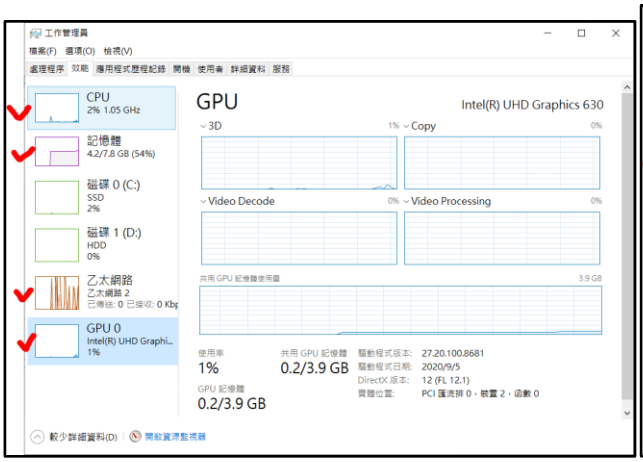

程式和功能
控制台 › 所有控制台項目 › 程式和功能
控制台首頁
檢視已安裝的更新
開啟或關閉 Windows 功能
解除安裝或變更程式
若要解除安裝程式，請從清單選取程式，然後按一下 [解除安裝]、[變更] 或 [修復]。
組合管理 解除安裝
名稱 發行者 安裝於 大小 版本號
ESET Endpoint Security ESET, spol. s r.o. 2020/8/12 210 MB 7.3.2039.0
ESET Management Agent ESET, spol. s r.o. 2020/8/12 167 MB 7.2.1266.0
CDBurnerXP CDBurnerXP 2020/8/11 18.9 MB 4.5.8.7128
Microsoft Visual Studio 2010 Express Prerequisites x64 - CHT Microsoft Corporation 2020/6/24 22.0 MB 10.0.40219
Microsoft SQL Server 2008 R2 管理物件 Microsoft Corporation 2020/6/24 14.3 MB 10.50.1750.9
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6... Microsoft Corporation 2020/6/24 10.1 MB 9.0.30729.6161
Microsoft SQL Server System CLR Types Microsoft Corporation 2020/6/24 951 KB 10.50.1750.9
Microsoft Visual Studio 2010 ADO.NET Entity Framework Tools Microsoft Corporation 2020/6/24 55.1 MB 10.0.40219
Microsoft Visual C++ 2010 x86 Runtime - 10.0.40219 Microsoft Corporation 2020/6/24 25.2 MB 10.0.40219
Microsoft Visual C++ 2010 x64 Runtime - 10.0.40219 Microsoft Corporation 2020/6/24 33.4 MB 10.0.40219
Microsoft Corporation 產品版本: 9.0.30729.6161
大小: 10.1 MB

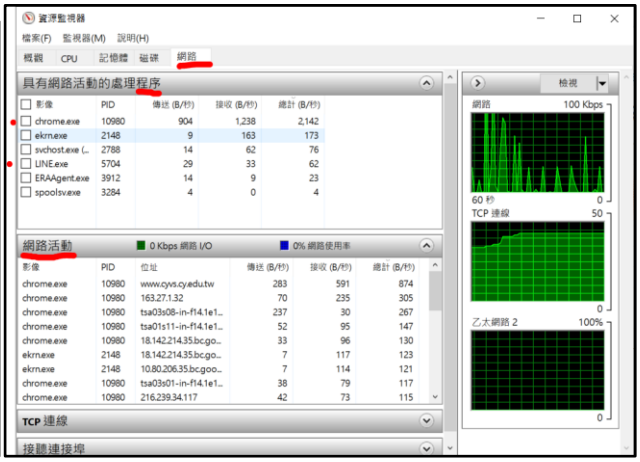

設定
首頁
尋找設定
系統
平板
多工
投影到此電腦
共用體驗
剪貼簿
遠端桌面
關於
遠端桌面
遠端桌面可讓您使用遠端桌面用戶端應用程式 (適用於 Windows、Android、iOS 和 macOS)，從遠端裝置連線到這部電腦並加以控制。然後，您就可以從另一部裝置工作，如同直接在這部電腦上工作一樣。
啟用遠端桌面
關閉
使用者帳戶
選取可以從遠端存取此電腦的使用者
來自網站的說明
設置遠程桌面
取得協助
提供意見反應


系統內容
電腦名稱 硬體 進階 系統保護 遠端
遠端協助
允許到這部電腦的遠端協助連線(R)
如果我啟用遠端協助會有什麼影響?
進階(V)...
遠端桌面
選擇一個選項，然後指定可以連線的人員。
不允許遠端連線到此電腦(D)
允許遠端連線到此電腦(L)
僅允許來自執行含有網路層級驗證之遠端桌面的電腦進行連線 (建議)(N)
協助我選擇
選取使用者(S)...
確定
取消
套用(A)

六、檢視電腦資源運行狀況

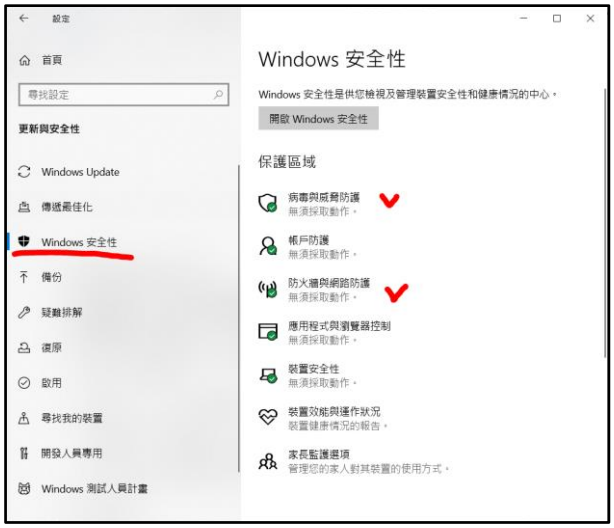
1. 檢視電腦資源運用，排除惡意軟體及挖礦軟體
   A. 惡意軟體通常是資安的一大隱憂，可藉由防毒軟體、防火牆進行防範，但仍需多留意自身電腦的狀況，如發現異常，應儘速處理或通報。
   B. 挖礦軟體則會佔用電腦大量資源(網路流量、CPU、GPU 運算能力及電力)。
   C. 工作管理員/效能：搜尋「**工作管理員**」或直接執行 **taskmgr**
   D. 檢視「較多詳細資料」，並切換到「效能」頁籤，可看到電腦中各種運算資源執行狀況，說明如下
      (1). **CPU** 是電腦主要運算元件，通常會高高低低跳動，但如果連續高使用率(接近 100%.)，可能有異常…
      (2). **GPU** 是顯示卡的運作單元，通常處於低使用率。(挖礦程式也會偷用)
      (3). **記憶體**通常會保持穩定狀態，開越多程式，用的記憶體越多。
      (4). 磁碟機通常也處於低使用率，除非是大量複製檔案、多媒體(繪圖、影片)剪輯…
      (5). 網路視使用情況而定，但長時間大流量的話也是屬於異常現象
      (6). 如果覺得異常，可以先從「**開啟資源監視器**」看到是哪些程式在使用這些資源，作為初步檢查。
   E. 覺得電腦變慢，或經常檢視電腦運作狀況，可能發現異常，進而避免受駭。
2. 使用 Process Explorer (進階)
   A. 下載 https://learn.microsoft.com/zh-tw/sysinternals/downloads/process-explorer
   B. 微軟提供的進程管理員，可以結合 VirusTotal.com 查驗電腦中的 process。

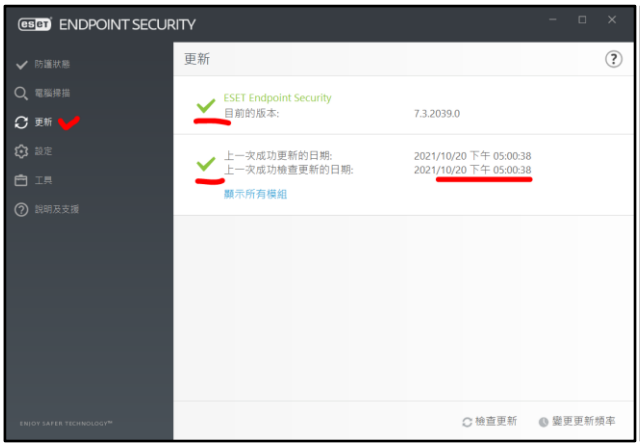


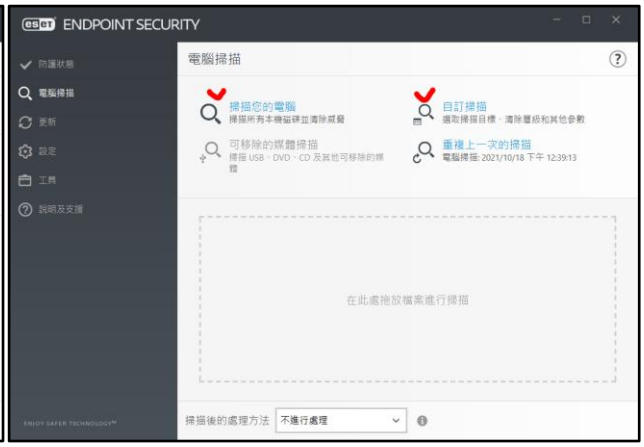


七、安裝防毒軟體及防火牆軟體

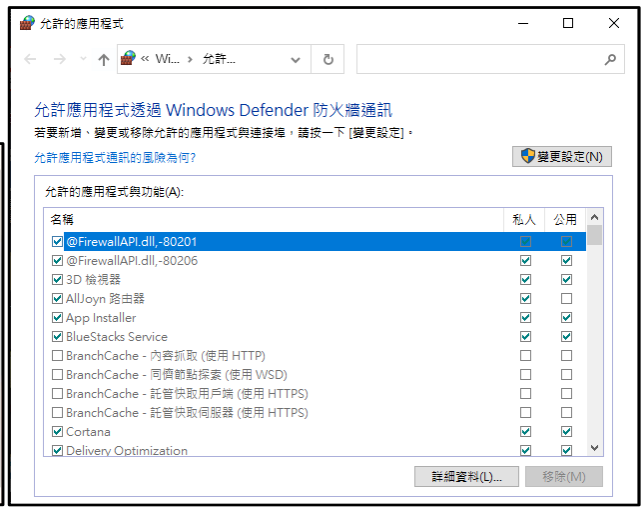
1. 首先搜尋「**Windows 安全性設定**」，確認各項目是否安全。
2. 校內建議擇一使用 **(1)ESET Endpoint Security 授權軟體 (2)Microsoft Defender & Firewall**
3. **校內電腦不建議自行安裝免費版防毒軟體，這通常只授權個人或家庭使用，並未授權機關、學校使用，一定要看清楚授權範圍。**
4. 安裝 ESET Endpoint Security 請向圖書館申請。(三年授權版，爾後可能需要安裝新版)
   A. 搜尋「**ESET Endpoint Security**」，檢視防護狀態、進行更新
   B. 在「**設定**」頁籤處檢查**電腦**、**網路**是否均正常啟用。
   C. 檢視模組更新狀態，通常每日都有更新檔，如果很多天沒更新，可能是有狀況了。
   D. 電腦掃描：進行電腦全機掃描或手動選擇要掃描的範圍
      (1). 使用「掃描您的電腦」進行全機掃描，需花比較久的時間
      (2). 使用「自訂掃描」擇要掃描，如重要資料或新下載的檔案
      (3). 使用「可移除的媒體掃描」進行隨身碟、光碟…等
   E. 進行全機掃描時，掃描期間會大量存取硬碟，可能會影響電腦的運作速度，並需要較長的時間，建議選擇空檔時間進行。
5. 使用 Windows 10 **內建 Defender 及 Firewall**
   A. 搜尋「**Windows 安全性**」，檢視是否均為綠色打勾狀態。
   B. **病毒與威脅防護**：defender 防毒程式，請
      (1). 掃描選項：可進行快速掃描、完整掃描、自訂掃描 (參考上方 ESET 說明)
      (2). 檢查更新：預設會自動更新，請確認已更新至最新。
   C. **防火牆與網路防護**：
      (1). 允許應用程式通過防火牆：可檢視目前可自由進出防火牆的程式。這裡應該要移除可疑、不明的應用軟體或程式，拒絕這些程式進出防火牆，降低風險。
      (2). 進階設定：會開啟防火牆規則設定程式**(需要較專業的知識)**
   D. 注意：若有安裝 ESET 會取代 Windows 內建防毒及防火牆，畫面會不一樣。







底下是 Windows10 Defender 操作畫面



八、關閉自動播放 AutoRun 及檢視開機啟動自動執行 Startup

1. 外接式媒體如 USB、CD、硬碟連接到電腦後，預設會使用自動播放功能，直接執行媒體中設定的自動執行程式(autorun.inf，如開啟安裝程式，自動播影片、歌曲…)，常被利用來自動執行惡意程式，造成電腦感染，關閉自動播放功能可以減低風險。

2. 搜尋「自動播放設定」，關閉「為所有媒體與裝置使用自動播放功能」。

3. 搜尋「工作管理員」或在工作列上按滑鼠右鍵啟動工作管理員

   A. 切換到「開機」頁籤，這裡會顯示開機時自動執行的程式，可檢視是否有不明軟體

   B. 介紹幾個**可能**出現在學校行政電腦的軟體，以免誤刪

      (1). CheckServer.exe 是自然人憑證用的跨元件平台，使用憑證時，常會安裝 HiCOS 和這個，可參考內政部憑證中心說明：https://moica.nat.gov.tw/download_1.html

      (2). DSICStarter：公文系統跨瀏覽器元件，使用電子公文時會安裝

      (3). 公文製作通訊錄壓縮及同步工具程式，舊版電子公文用的工具程式。(用不到了)

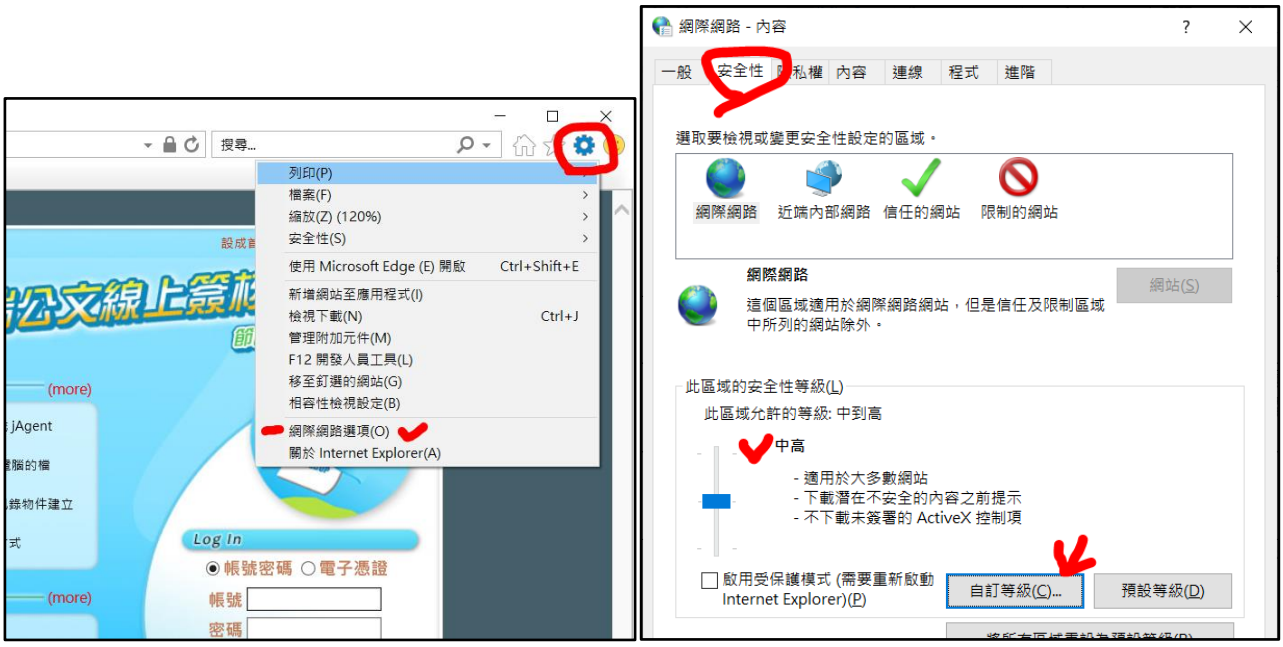
      (4). ESET，有安裝學校防毒軟體，開機都會看到大的 Logo 跳出來

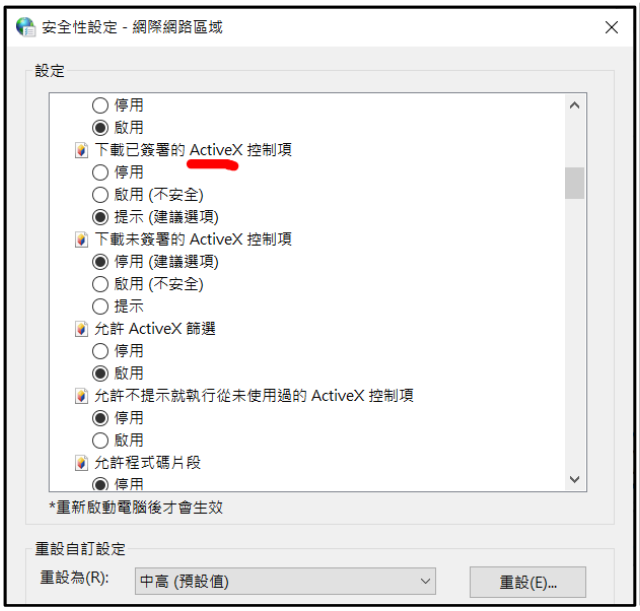
      (5). 其他 Intel…、Audio…通常是 CPU 或音效卡驅動，保留。

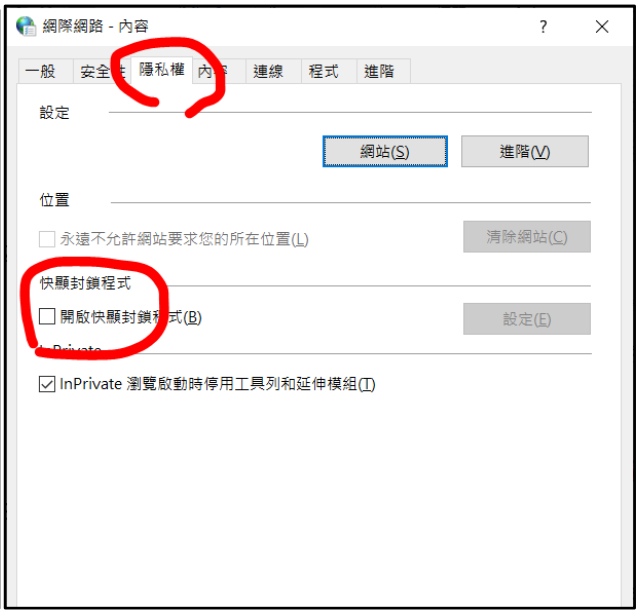
九、完成瀏覽器安全設定

1. 時代的眼淚：IE 是早期許多行政系統綁定的瀏覽器，即時不斷更新版本但仍需使用相容性設定來使用這些系統，這麼多年了，也真的該退出舞台了，微軟宣佈 IE11 於 2022 年 6 月 15 日終止支援，IE 系列不應該再出現了。即使目前尚在使用 IE，仍需設定好瀏覽器的安全設定。

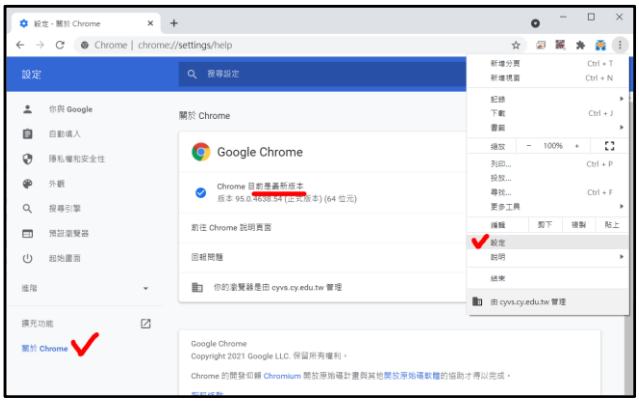
2. IE 安全性設定：搜尋「網際網路選項」或由 IE 進入，選取「**安全性**」頁籤
   A. **安全等級**請設定為「**中級**」或更高，並關閉快顯功能、ActiveX 等主動執行功能及封鎖彈跳視窗，某些系統須降低安全性或需加裝外掛功能，請先進行安全檢查及管理。
   B. 停用 ActiveX 功能會影響大多數綁定 IE 的系統，部份系統會有相容性、或需加裝外掛功能等要求，請先進行安全檢查及管理。**但建議停止使用綁定 IE 瀏覽器的系統**。
3. Chrome 安全性設定： Chrome 視窗，右上角「…」進入設定頁面
   A. 檢查版本：網址列直接打上「**chrome://settings/help**」，確認為最新版本
   B. 隱私權及安全性：網址列直接打上「**chrome://settings/ privacy**」
      (1). 設定安全性：至少為「標準防護」以上
      (2). 網站設定：可設定或檢視已開放網站權限，請關閉/移除不必要的權限。
4. Edge 安全性設定：Edge 視窗，右上角「…」進行設定頁面
   A. 檢查版本：網址列直接打上「**edge://settings/help**」，確認為最新版本
   B. 隱私權、搜尋與服務：網址列直接打上「**edge://settings/ privacy**」
      (1). 隱私權的設定請依自己需求或依預設值設定
      (2). 安全性請確認**開啟 Microsoft Defender SmartScreen**、**封鎖潛在的垃圾應用程式**。

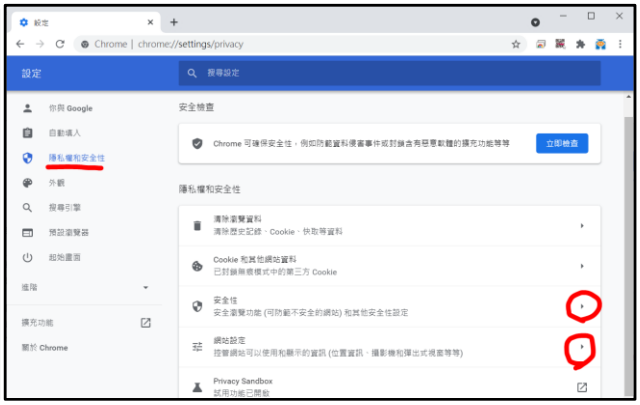


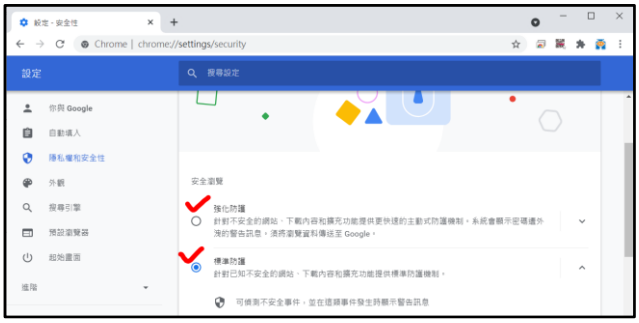




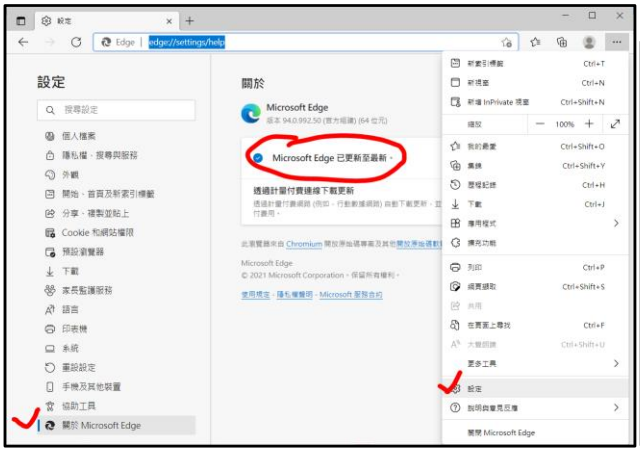
底下是 Chrome 設定畫面

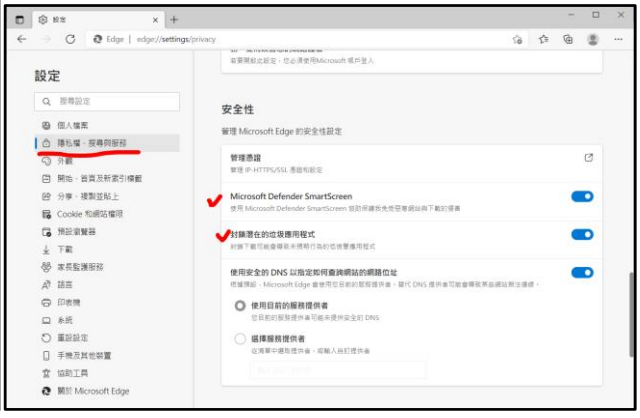






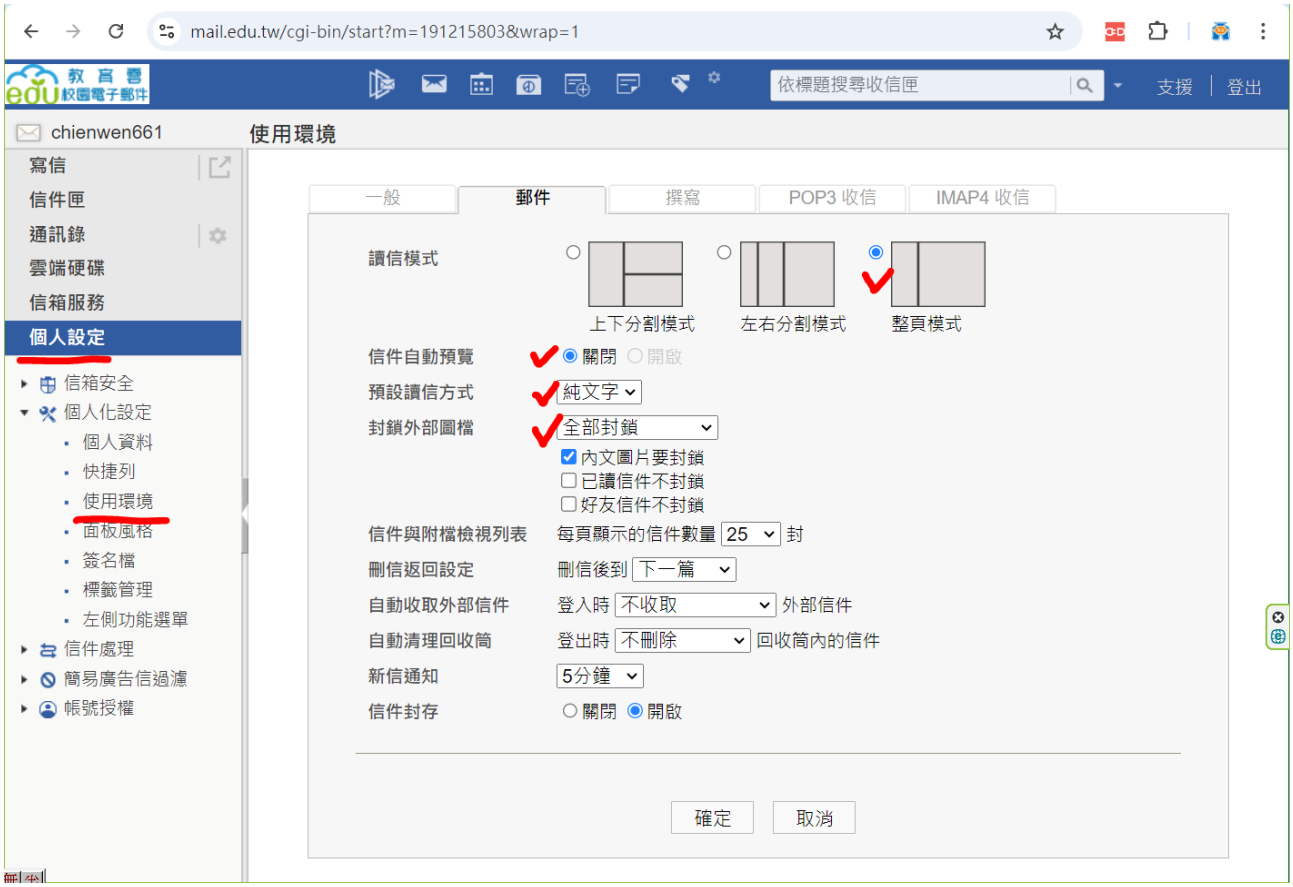
底下是 Edge 設定畫面





十、關閉郵件已關閉信件預覽

1. 使用信件軟體如 Outlook 收信時，預覽信件內容含 HTML 格式(含圖片、連結、指令…)容易造成中毒等情況，因此建議關閉
   A. Outlook 設定關閉預覽信件：請參考 Microsoft 說明文件，搜尋【使用和設定 [讀取窗格] 以預覽郵件】，或點選連結 https://support.microsoft.com/zh-tw/office/%E4%BD%BF%E7%94%A8%E5%92%8C%E8%A8%AD%E5%AE%9A-%E8%AE%80%E5%8F%96%E7%AA%97%E6%A0%BC-%E4%BB%A5%E9%A0%90%E8%A6%BD%E9%83%B5%E4%BB%B6-2fd687ed-7fc4-4ae3-8eab-9f9b8c6d53f0
   B. Outlook 設定以純文字讀取信件內容：請參考 Microsoft 說明文件，搜尋【以純文字讀取電子郵件】，或點選連結 https://support.microsoft.com/zh-tw/office/%E4%BB%A5%E7%B4%94%E6%96%87%E5%AD%97%E8%AE%80%E5%8F%96%E9%9B%BB%E5%AD%90%E9%83%B5%E4%BB%B6-16dfe54a-fadc-4261-b2ce-19ad072ed7e3
   C. 教育雲電子郵件信箱安全設定：【左側選單/個人設定/個人化設定/使用環境】，點選【郵件】頁籤，【信件自動預覽設為關閉】及【預設讀信方式設為純文字】



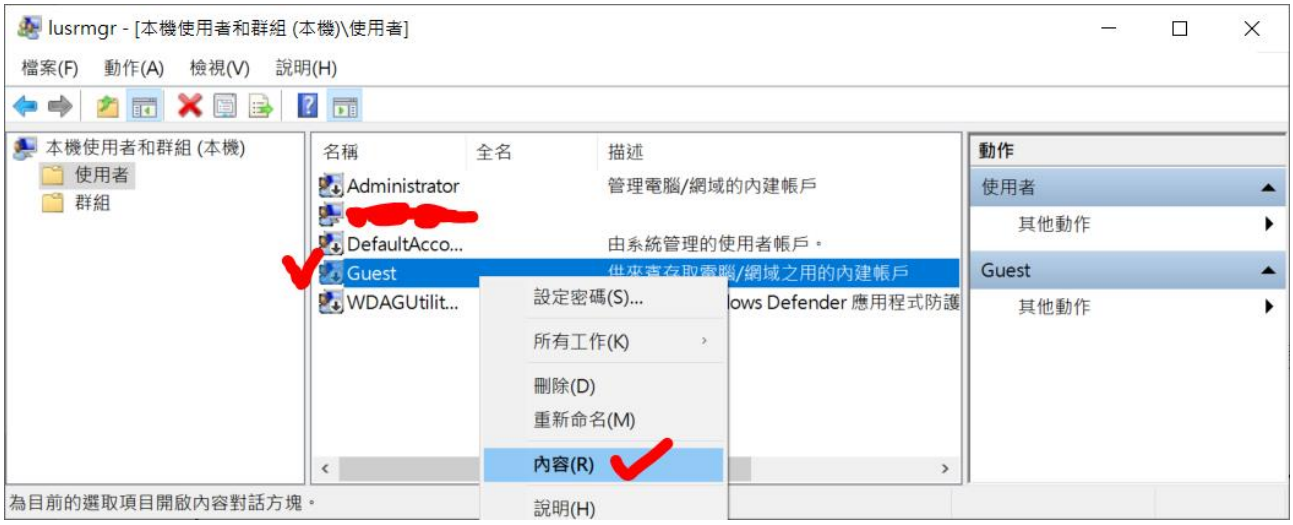
2. 公務使用教育雲端電子郵件，**不建議設定自動轉寄至其他系統**(如 gmail)，容易誤點社交工程信件。建議**使用電腦版收信，手機請安裝 Mail 2000 收信程式**。

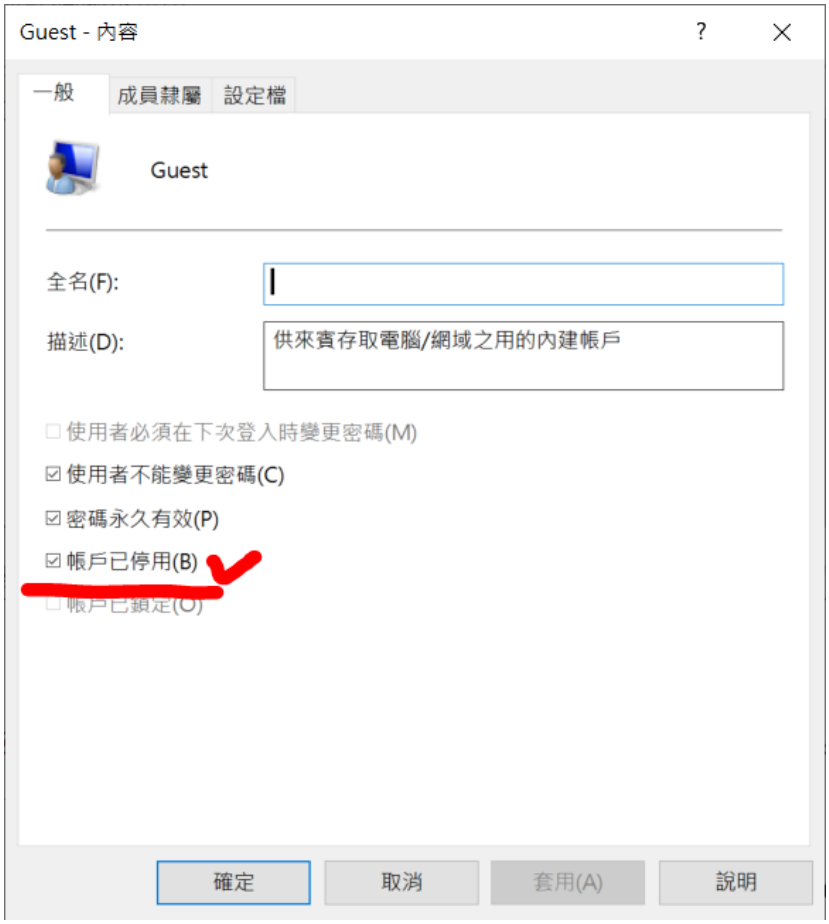
十一、關閉 Guest 帳號

1. 本項次在檢核表中已刪除，請配合「一、密碼安全性設定及密碼設定」操作時檢查並確認 Guest 帳號保持停用狀態即可。
2. 和第一項設定帳號密碼的操作一樣

   A. 本機使用者和群組：搜尋「**電腦管理**」或直接執行 **lusrmgr.msc**

   B. 選擇「**本機使用者和群組**」下的「**使用者**」，在視窗中間找到 **Guest**，按滑鼠右鍵選單，點選**內容**，確認【**帳戶已停用**】已打勾。





十二、隔離機密性敏感檔案資料

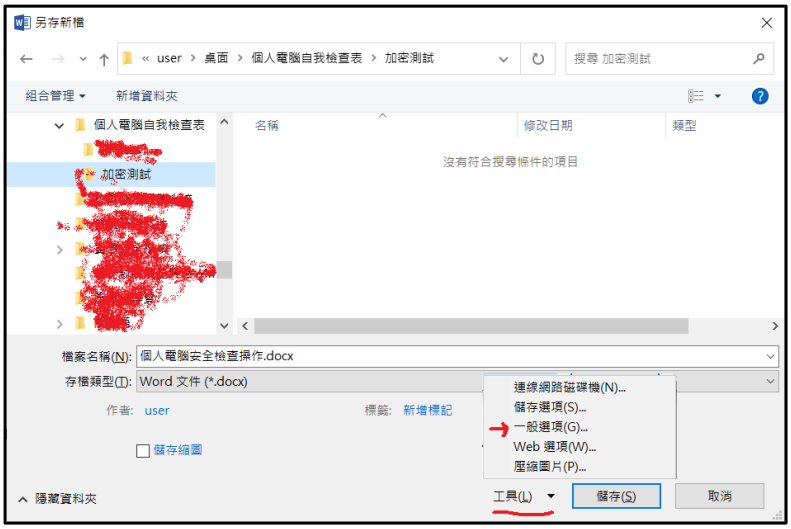
1. 應進行 (1)機敏檔案設定加密密碼，(2)機敏檔案應進行實體隔離
2. 機敏檔案加密：
   A. PGP 加密：GnuPG 是自由軟體，且採用非對稱式公私鑰方式加密，安全性較高，也適合檔案傳遞。需要透過網路傳遞資料時，是比較安全的做法。
      (1). 每人自己產生一對自己的金鑰，分別為公鑰及私鑰，**公鑰可以散佈**，私鑰則需妥善保密保存。(自己也可以產生很多組公私鑰…)
      (2). 使用自己的公鑰加密自己的檔案，只有自己的私鑰可解開。
      (3). 傳遞檔案 1：取得並使用 A 君的公鑰加密檔案，則此檔案只有 A 君的私鑰可解開，適用於傳檔案給 A 君。
      (4). 傳遞檔案 2：A 君使用你的公鑰加密檔案，只有你的私鑰可解開，適用於 A 君傳檔案給您。
      (5). 缺點：**加密操作比較複雜**，需安裝 GPG4Win 軟體
      (6). MODA Writer 可以使用 PGP 進行加密。
      (7). GUNPGP 網站：https://www.gnupg.org/index.html

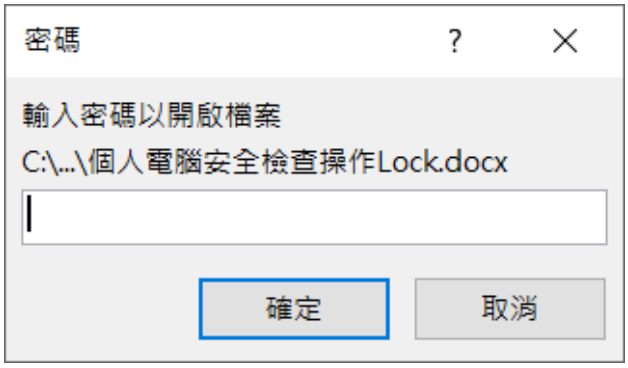
   B. 單一密碼保護：

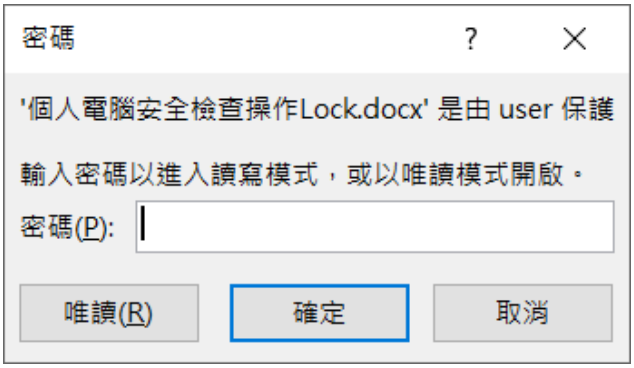
      (1). Office 文件(Word、Excel…)及 ODF 文件在存檔時可以指定保護密碼，**一檔一密碼**
         a. 以 Word 為例：新檔儲存或**另存新檔**時，點選底下的「**工具/一般選項**」，可以輸入「**保護密碼**」及「**防寫密碼**」，說明如下
            1. 「保護密碼」在開啟檔案時會要求輸入密碼，密碼錯誤不會打開檔案
            2. 「防寫密碼」旨在防止改動內容，所以即使不知道密碼，也可以唯讀方式看到內容，只設定防寫密碼並**無法達到保密效果**。
         b. 以 MODA ODF Application Tools Writer 為例：和 Word 一樣，另存新檔時，下方存檔選項，勾選「**使用密碼儲存**」，這裡稱之為「**檔案加密**」與「**檔案共享**」。
         c. 上述加密方式，每個檔案皆個別加密，安全性高，但檔案多時較沒效率。
         d. Word 和 Writer 轉存為 PDF 時也可以設定保護密碼，請參考圖解。
      (2). **使用壓縮軟體**，壓縮後加密，資料檔案本身未加密，但解壓縮檔需要輸入密碼
         a. 建議使用 **7-Zip** 進行檔案的壓縮及資料夾的加密，7-Zip 採用 GNU LGPL 授權，任何人都可以免費使用。https://www.7-zip.org/
         b. 下載安裝後，在檔案或資料夾上**按右鍵**，選單 7-Zip 中點選「**加入壓縮檔…**」，對話視窗中可**輸入加密密碼**。
         c. 加密後的壓縮檔，按右鍵選擇「**解壓縮檔案**」時，**需要輸入密碼**才能解開。
         d. 使用壓縮軟體可針對整個資料夾加密，但解壓縮才需要密碼，個別檔案並未加密，安全性較低，比較適合用在傳遞檔案時加密，或檔案封存時加密。
      (3). 並非檔案加密後就安全了，密碼太簡單或密碼洩漏仍有風險，因加密方式的關係，有人人士強行破解的機會也是不低，要注意多方面的資料保密措施。
3. 實體隔離
   A. 使用可攜式媒體，如隨身碟、外接式硬碟等方式保存機敏檔案，需使用時再接上電腦，編輯完後則立刻離線，並使用各種保護措施妥善保存，如人員管制、門禁管制、

櫃子上鎖、加密碟...

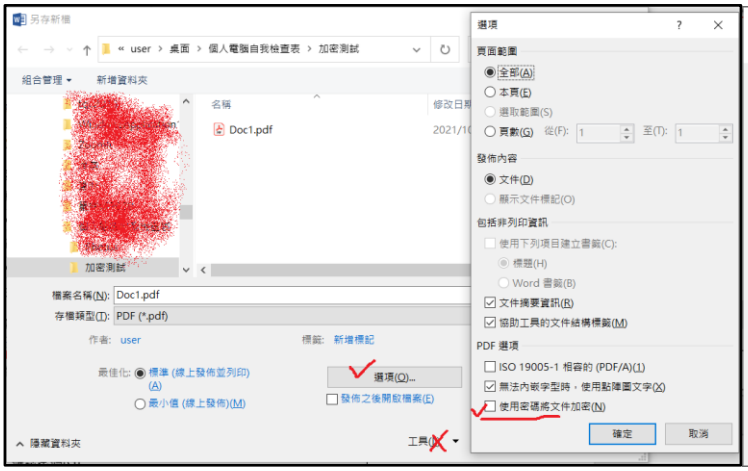
底下是 Microsoft Office Word 的操作

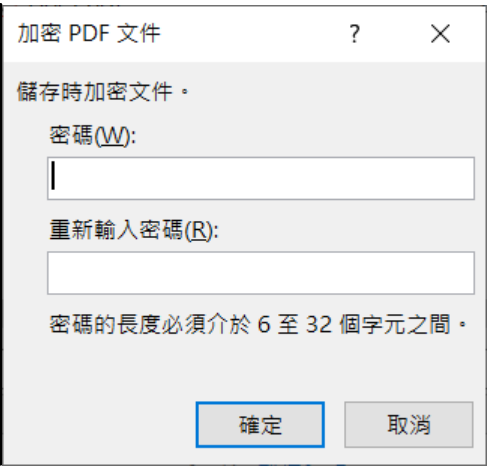


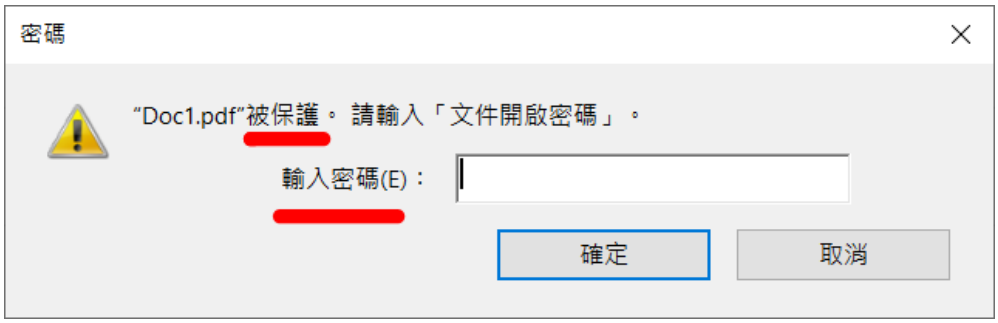




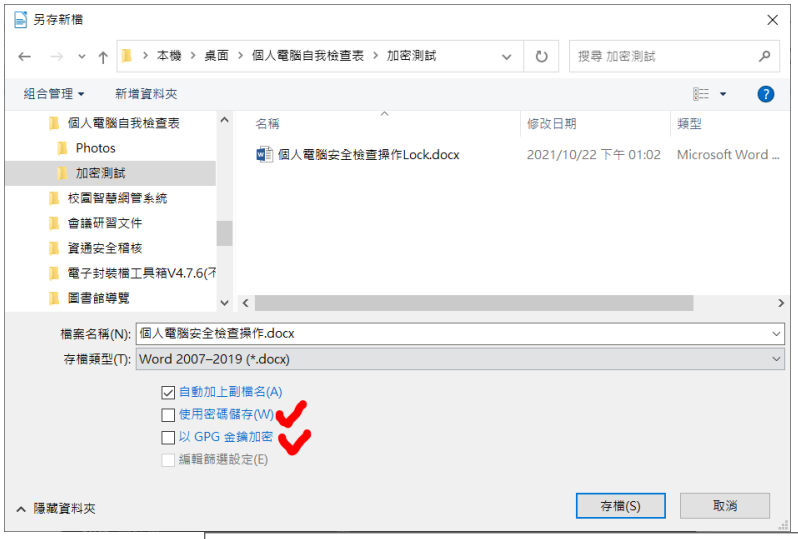
Word 轉存 PDF 檔時，設定加密

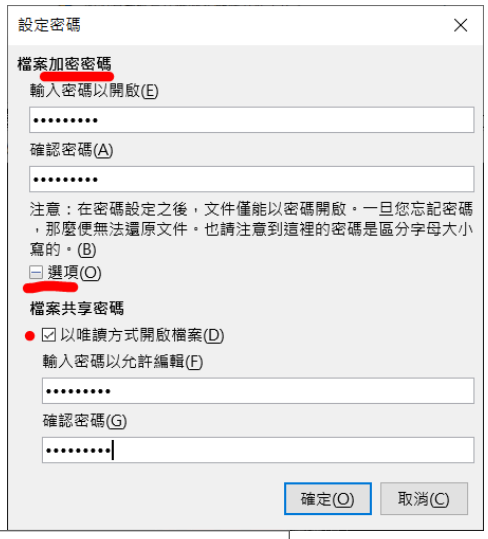


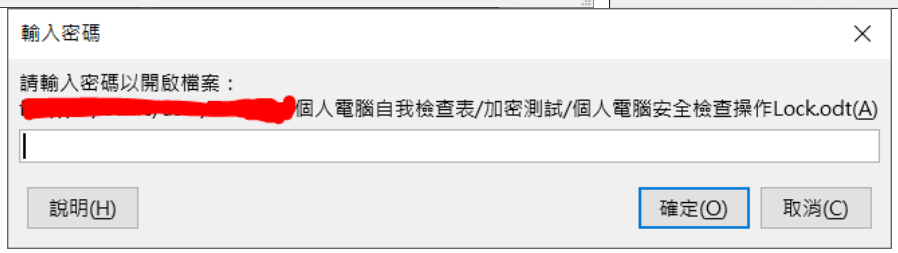




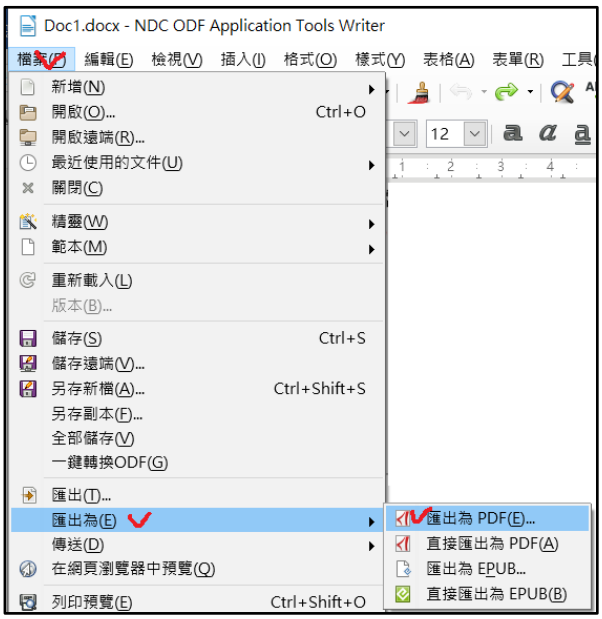
底下是 MODA ODF Application Tools Writer 的操作畫面

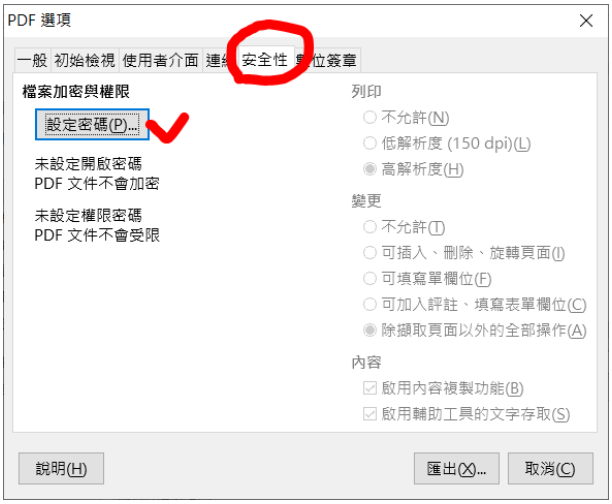




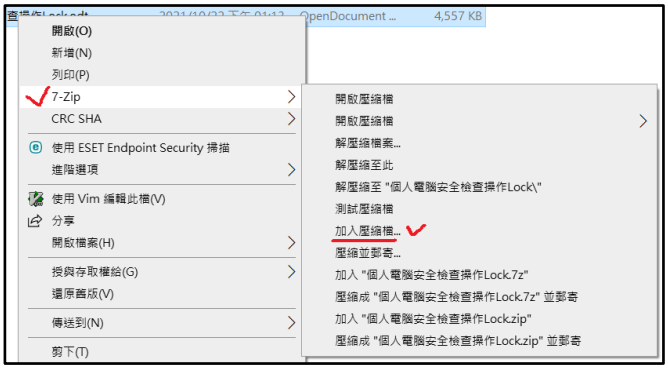


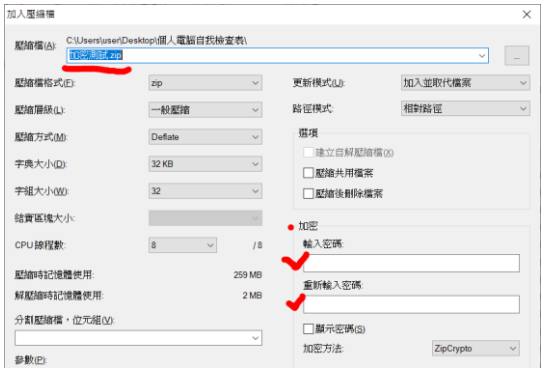
底下為 Writer 匯出為 PDF 時設定保護密碼





底下是 7-Zip 設定密碼的操作



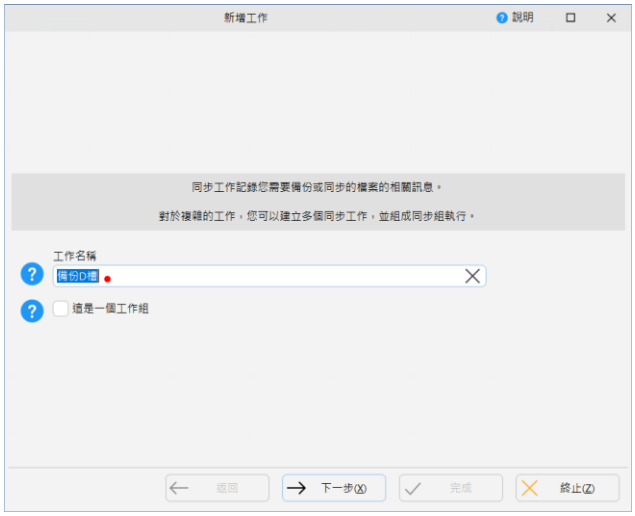


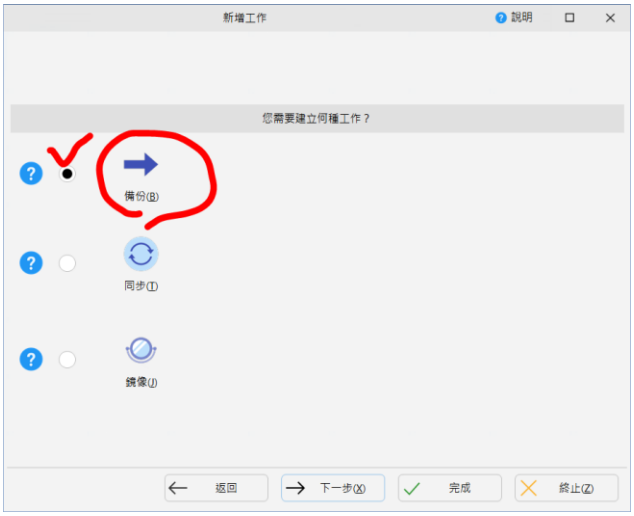
十三、資料備份

1. 準備 **(1)了解備份原則，訂定備份計畫，(2)準備備份媒體，(3)手動備份或使用備份軟體**
2. **3-2-1 備份原則**：至少三份備份，存放在兩種不同儲存媒體，至少一份異地保存。
3. 備份計畫：**應依個人公務資料處理量擬定個人備份計畫，至少每學期進行一次完整備份(建議每個月一次)**。備份計畫中應考量，備份哪些資料？多久備份一次？備份在哪裡？怎麼備份？機敏資料如何保密？
   A. **備份資料**：**先確認自己電腦中哪些資料要備份**，這些資料放在電腦中的哪裡？最好記錄下來。平時個人電腦資料整理很重要，資料整理得好，比較不容易漏掉。
   B. **備份時機**：通常分定期備份及即時備份，**定期備份完整資料**，**即時備份重要資料**。定期備份如每學期(或每一個月)備份所有資料，每週(或每天)備份有變更過的資料。即時備份則是針對目前處理的資料，很重要而且不斷修改中，可利用**版本控制**的方式進行即時備份。
   C. **備份媒體及位置**：
      1. 除了在自己電腦(本機)備份外，應該在**隨身碟/外接式硬碟/雲端硬碟**等**本機以外**的媒體進行備份，定期備份也可考慮使用**光碟片**…。
      2. **要減少資料外洩或毀損的風險**，外接式設備**不應該隨時插在電腦**上，要用時再接上，不用時移除，接在電腦上的時間越久風險越高。**機敏資料及不公開之公務資料檔案不應備份於外部雲端系統**。若使用校內雲端備份要加強雲端設定的資安問題。另外考慮**外接式設備容易故障**、遺失，所以老舊媒體換新、備用的問題也應列入考慮。
      3. **儲存媒體的放置地點**應考慮防塵、防火、防水、防盜、保密等安全性。至少一份異地保存(另一間辦公室、另一棟大樓、甚至另一個縣市…)，才能避免大型災難，同一地點所有資料均毀損的風險。
   D. 備份方式：
      1. 資料量不多時，可以**手動備份**，打開檔案總管，利用複製檔案的方式備份。
      2. 資料量較多時，可以利用**備份軟體**自動進行
         a. 隨身碟或外接式硬碟等廠商都附贈有修復軟體及資料備份軟體，有些附在硬碟中，有些需自行上網下載，優點是功能完整，缺點是可能只適用該廠牌設備。
         b. 備份軟體：**請自行選擇合適的備份軟體**，底下以 SyncBackFree 做為操作範例，SyncBackFree 免費版符合簡易備份功能，授權教育單位、政府機關免費使用，有中文介面。
            1. 下載 https://www.2brightsparks.com/download-syncbackfree.html
            2. 簡易操作流程參考後面圖解
   E. 備份資料存放：遵求上 3-2-1 原則妥善保存，機敏資料應加強管理及管制。
   F. 備份資料應定期進行備份還原演練，確保備份資料可以有效還原，尤其是資訊系統、資料庫的備份資料，應訂定備份還原演練計畫。

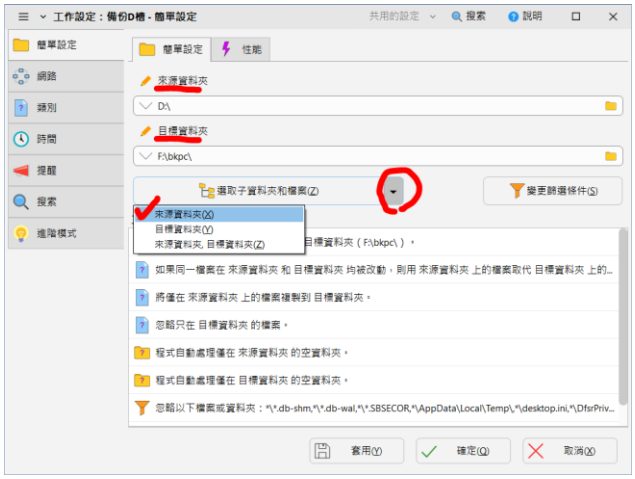
SyncBackFree 操作圖解

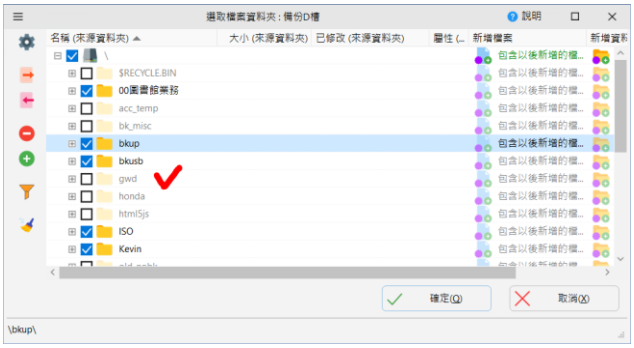
●左下角新增一個工作，備份硬碟 D 槽中的資料 (1)命名 (2)備份 (3)壓縮否？ (4)進入設定

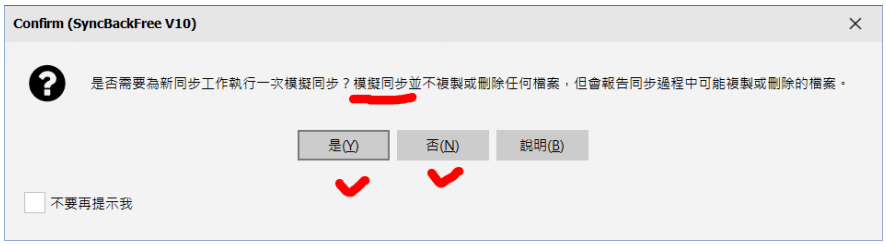




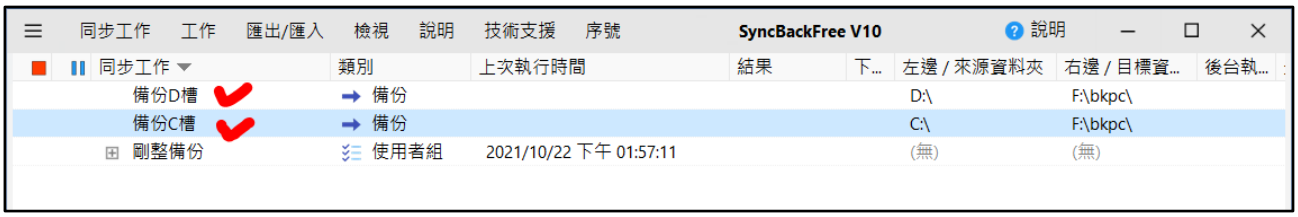
(5)選擇備份來源資料夾、目的地(外接硬碟) (6)勾選要備份的來源資料夾 (7)模擬嗎？都可



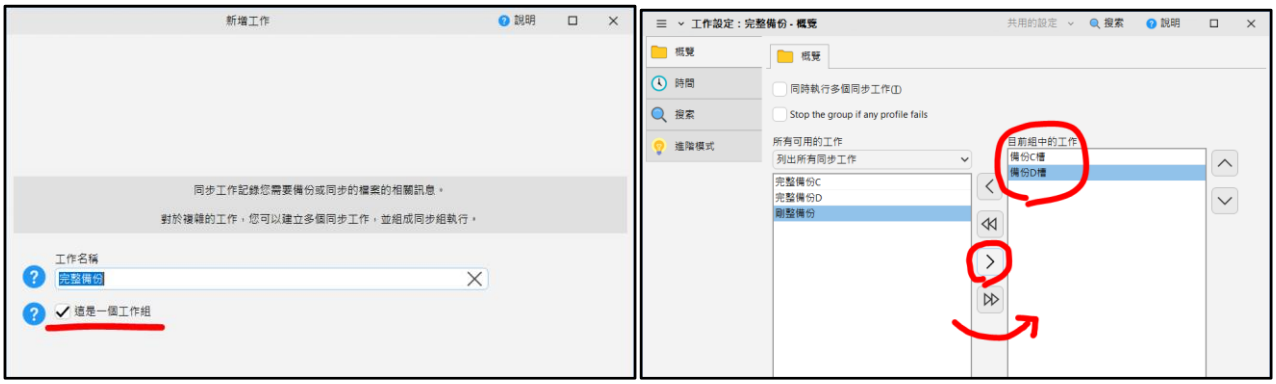


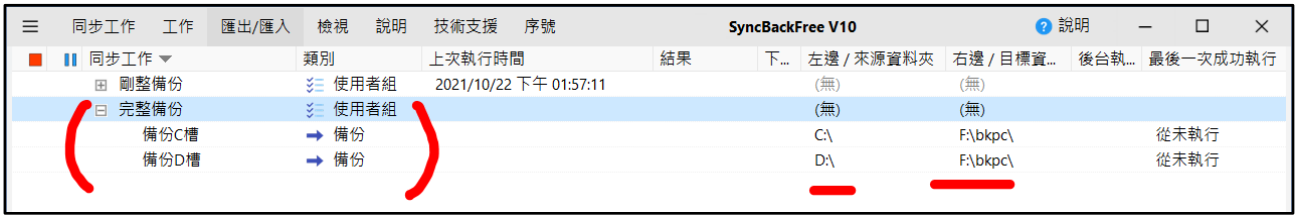


(8)以相同方式再建立備份 C 槽的設定檔，C 槽大多數的資料在 C:\Users\user 底下，Desktop 桌面、Documents 文件、Downloads 下載、Favorites 我的最愛、Pictures 圖片…或者整個 C:\Users\user 全備份。

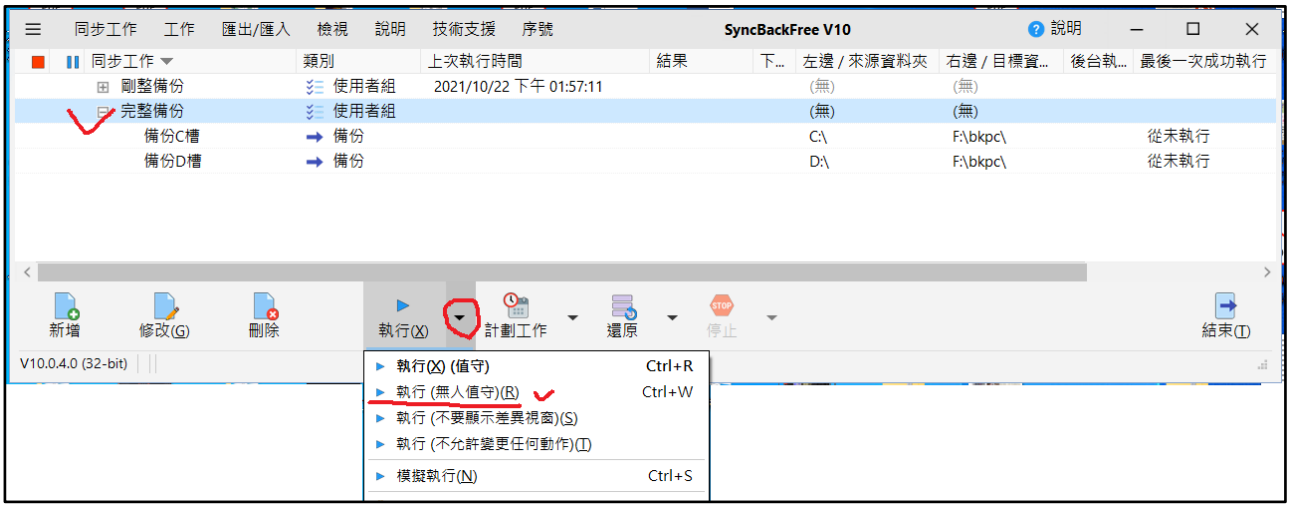


(9)建立備份工作組，把剛剛兩個備份工作組合在一起。如果有其他磁碟一樣加進來。

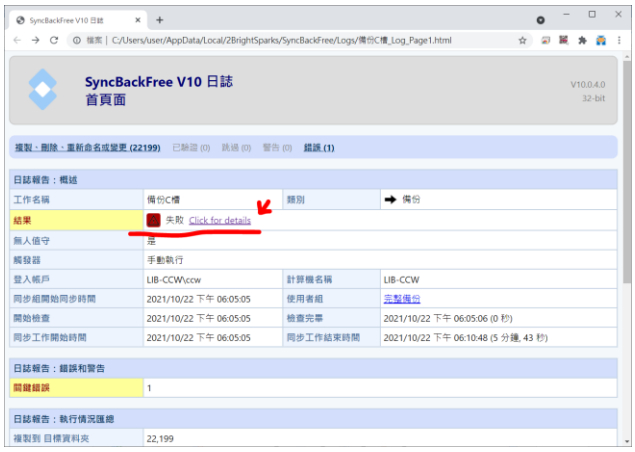




(10)開始備份-無人值守模式會默默備完，備份期間最好不要開啟任何檔案…



(11)備份結果會記錄在日誌，可查明備份錯誤的部份及原因



(12)出現錯誤，可關閉所有已開啟程式及檔案，再進行一次備份(已備份過的檔案，檢查後不會重新複製，所以時間不會太久)