彰化縣立陽明國中108年管理審查會議紀錄簽到表

壹、 時間：108年7月22日 8：30分

貳、 地點：校長室

參、 主席：余立焜校長

單位職級	組別	職掌事項	簽到	備註
校長 (資通安全長)	策略規劃組	執掌事項詳列於本校資通安全管理計畫中	余立焜	
教務主任 學務主任 總務主任 輔導主任	資安防護組	1.資通安全政策及目標之研議。 2.訂定機關資通安全相關規章與程序、制度文件，並確保相關規章與程序、制度合乎法令及契約之要求。 3.依據資通安全目標擬定機關年度工作計畫。 4.傳達機關資通安全政策與目標。 5.其他資通安全事項之辦理與推動	蔡志鏡 鄭瑜如 楊太元 許祐偉	
人事主任	績效管理組	辦理資通安全內部稽核	陳政輝	
教師兼任 資訊組長 教師兼任 設備組長	資安管理組	1.資訊組長兼任策略規劃組顧問，並辦理資通行政業務，系管師協辦。 2.資通安全技術之研究、建置及評估相關事項。 3.資通安全相關規章與程序、制度之執行。 4.資訊及資通業務之盤點及風險評估。 5.資料及資通業務之安全防護事項之執行。 6.資通安全事件之通報及應變機制之執行。 7.其他資通安全事項之辦理與推動。	陳炳訓	

彰化縣立陽明國中108年管理審查會議紀錄

壹、 時間：108年7月22日 7：30分

貳、 地點：校長室

參、 主席：余立焜校長　　紀錄：陳炳彰老師

肆、 出席人員：如簽到表

伍、 業務報告：

今年度第一次將資訊安全列入重點實施工作，將各單位依資安分為A-E級，本校暫列至C級，若將網頁主機移至縣網中心即可降至D級，目前朝此方向努力。

陸、 討論事項：

案由一：過往管理審查之議案的處理狀態。

決　議：因今年為首年執行資安法要求事項之管理審查會議，故無過往管理審查之議案的處理狀態。

案由二：資通訊安全或個資管理要求的變更，如上級機關要求、最高行政管理會議決議事項。

決　議：資安法於108年1月1日開始施行，故本校今年按照資安法D級機關要求事項辦理相關業務。

案由三：管理目標與指標量測結果。

決 議：針對維護計畫中

二、資通安全目標訂定的目標審視今年是否有達到目標

1. 本校知悉資安事件發生，於規定的時間完成通報、應變及復原作業。
2. 本校108年資安事件等級3或4級次數為0次，達到本校訂定的目標。
3. 本校108年資安事件等級1或2級次數為2次，達到本校訂定的目標。

案由四：內外部稽核結果及持續改善之機會。

決　議:107年度本校ISAS的報告印出後提出改善的方法(如案由四附件)

案由五：資安事故與不符合項目之矯正情形。

決　議:317同學下載遊戲體 內夾帶挖礦程式，IP來源俄羅斯

（詳如案由五附件）

案由六：風險評鑑結果及風險處理計畫執行進度。

決　議:風險評鑑工作表中的風險值如果超過可接受風險如何去做改善?

因今年度為第一個實施年度，故請先在此訂定一個貴校可接受的風險值。

本校訂定可接受風險值為12，風險評鑑結果並無資產風險超過可接受風險/有(沒有資產超過)可接受風險值。

案由七：其他政策面須請示之資安管理事項。(例如:可接受風險值的變更，須請示明年是否採購某項設備降低風險等)

決　議:本校網頁主機在近期會移轉至縣網中心。

臨時動議：

1．　建議有機敏性資料可用彰化縣G-suite ，利用權限控制確保資料外流。

決議:一致通過。

散會。

(事件單編號:AISAC-161028)(告知通報)入侵事件警訊

收件匣

service 上午8:31 (6 小時前)

寄給 service

教育機構資安通報平台

事件類型:入侵事件警訊

事件單編號:AISAC-161028

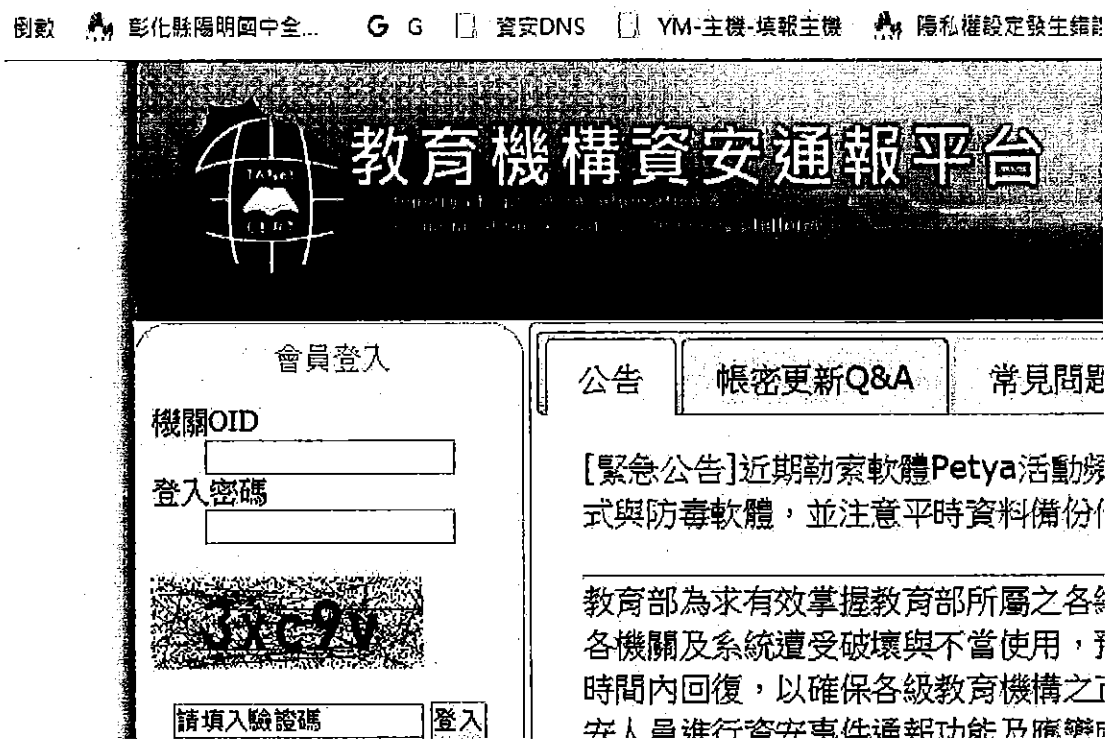
原發布編號	ASOC-INT-201902-0538	原發布時間	2019-02-21 08:31:05
事件類型	對外攻擊	原發現時間	2019-02-21 07:34:08
事件主旨	通報:[彰化縣立陽明國民中學]163.23.68.62 General.Interest: Monero.Cryptocurrency.Miner,		
事件描述	ASOC發現貴單位(彰化縣立陽明國民中學)所屬 163.23.68.62 疑似對外進行 General.Interest: Monero.Cryptocurrency.Miner, 攻擊		
手法研判	Monero(XMR)是一個創建於2014年4月開源加密貨幣，它可以在Windows、Mac、Linux和FreeBSD上運行。貴單位疑似對外進行非法攻擊行為，利用Monero挖礦惡意軟體進行採礦行為。Monero挖礦程序會吃掉受害機器的CPU運算能力，進而損耗受害機器系統資源。		
建議措施	惠請貴單位： 1.檢查防火牆紀錄：查看內部是否有開啟異常的連接埠。 2.利用工具程式(如:TCPview、procexp)於來源主機觀察，找出實際執行連線的程式，確認該程式是否為惡意程式。 3.若連線並非預期行為，則來源主機可能已遭植入惡意程式，建議利用木馬或後門清除程式掃瞄該主機，並手動檢測是否有惡意程式執行。 4.確實安裝修補程式並且更新系統。 5.攻擊名稱相關參考資料網站：https://fortiguard.com/appcontrol/44016 https://github.com/fireice-uk/xmr-stak-cpu https://en.wikipedia.org/wiki/Monero_(cryptocurrency)		
參考資料	無		
此事件需要進行通報，請 貴單位資安聯絡人登入資安通報應變平台進行通報應變作業			
如果您對此通告的內容有疑問或有關於此事件的建議，歡迎與我們連絡。			

教育機構資安通報應變小組
網址：https://info.cert.tanet.edu.tw/
專線電話：07-5250211
網路電話：98400000
E-Mail：service@cert.tanet.edu.tw

2019-221-06:26-58 172.20.113.17 電腦有挖礦行為 139.99.9.133:80

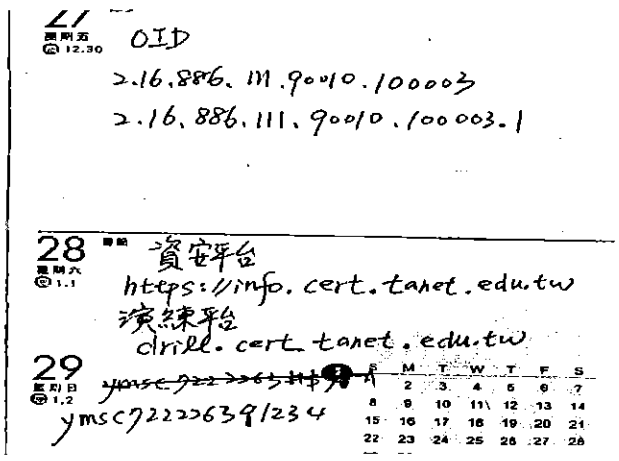
資安事件-通報程序

https://info.cert.tanet.edu.tw/prog/index.php



2.16.886.111.90010.100003.1

OLD



3. 設備資料：

ＩＰ位置：	172.20.113.17
網際網路位置：	163.23.68.62
設備廠牌、機型：	acer m4650G
作業系統：	Win10 64bit
受駭應用軟體：	
已裝置之安全防護軟體：	
	防毒軟體： Windows Defender 防毒軟體 防火牆： IPS/IDS： 其它：

4. 資通安全事件：基本資料

事件分類：	INT-對外攻擊-
破壞程度：	針對139.99.9.133:80有挖礦行為
事件說明：	1.已發現本校317蕭生在 https://steelraven7.itch.io/ravenfield下載遊戲 2.只要執行遊戲就會進行攻擊行為

◎緊急應變措施：

已中斷網路連線，待處理完成後再上線

解決辦法：

1.將系統重新安裝
2.告知該生老師及家長
3.封鎖並紀錄有問題網站 https://steelraven7.itch.io/ravenfield

彰化縣縣立陽明國民中學

資訊安全線上評量結果報告

製作日期：107 年 11 月 16 日

共用內容參考範本，請修改後儲存：

一、依據

教育部107年度提升校園資訊安全服務計畫之「教育機構個人資料保護工作事項」辦理。

二、目的

因應「個人資料保護法」實施、教育部「國中小學資通安全管理系統實施原則」、「教育部所屬機關及各級公私立學校資通安全工作事項」、本縣「中、小學資訊安全工作」及教育部年終視導等相關規定頒布，本局為了解各校資訊安全管理工作執行情形，特安排資訊安全稽核(內稽)及訪視作業，以協助各校建置資訊安全環境，落實資訊安全管理，以避免因疏忽而造成個人敏感性資料外洩，遭到不當利用而觸法，並使學校聲譽受損。

三、稽核項目

包含以下五大項，詳見「彰化縣政府教育局各學校資安訪視檢查表」。

(一)網路安全

(二)系統安全

(三)實體安全

(四)人員安全

(五)法令認知

四、稽核方式

第一階段：採學校自行內部稽核，相關資料請線上填報

由參與學校先依「彰化縣政府教育處各學校資安訪視檢查表」自評，於107年05月01日~07月19日期間，登入「全國中小學資安管理平台（http://isas.moe.edu.tw）」填報，並上傳相關佐證資料，供本局作線上審查。

第二階段：線上審查

由本單位相關承辦人員及資安輔導顧問進行線上審查。

第三階段：實地訪視

線上審查完畢後，辦理3天到校資安訪視(日期另行通知)，由教育局及資安顧問組成資安訪視團，自受稽學校中抽出4-6所進行到校訪查，確認線上審查項目落實程度。

五、稽核人員

各駐區督學、曾楚竣、白大川。

六、評定標準

訪視評定以「符合」、「部分符合」、「不符合」或「不適用」作為評比標準。

以下為評定標準定義：

(一)符合：

1. 實際作業依照書面規範進行；紀錄及審核皆按照規定辦理。

2. 已建立書面規範，但尚未有實際作業或紀錄。

(二)部分符合：

1.雖按照規範執行作業，但於過程中發生疏失或無相關書面紀錄。

2.作業流程尚有改善空間。

(三)不符合：

1.尚未規劃或執行相關安全管理規定。

2.違反自訂之管理規範。

3.違反教育部或本局之資安相關規範之要求。

(四)不適用：貴校之現行作業無相關作業需求。

七、線上評量結果：

(一)優點：

27項：宜設置滅火設備

(二)建議：

03項：無「無線網路存取」相關規範

20項：無「所有帳號註冊的記錄」

24項：無「通行碼設定規則之要求」

30項：有設備但無顯示溫濕度相關資訊

31項：無緊急照明設備

八、學校背景資料

序	項目內容	填答
01	貴校班級數(班)	50
02	貴校資訊、資訊安全人力概況(不含委外人力)(人)	1
03	貴校對外服務主機數量(台),包含實體主機、虛擬主機，不包含託管在教網的主機。	2
04	貴校行政電腦數量(台)	36
05	貴校班級電腦數量(台)	32
06	貴校電腦教室或專科教室用電腦數量(台)	107
07	貴校可攜式設備(公發的手機 平板 筆電)數量(台)	3
08	貴校對外連線頻寬(in/out，Mb)	300
09	校內個人電腦是否使用網路位址的轉址(NAT，Network Address Translation)?	是
10	貴校是否建置入侵偵測系統(IDS，Intrusion detection	否

	system)?	
11	貴校是否建置防火牆?	是
12	貴校是否建置防毒機制	否
13	貴校是否建置郵件過濾機制?	否
14	貴校重要的系統有哪些，請列出系統名稱	DNS WWW 學籍系統
15	貴校教職員工人數(人)	140

九、線上評量檢查表

受評量單位：彰化縣陽明國中　評量人員：何奇芳-國立暨南國際大學　評量日期：107年11月16日
自評結果：66分　　評量結果：59分

評量項目	自評	評量結果	執行現況或改善建議
一、資通安全管理規範			
01.訂定學校資通安全管理規範且經校長簽核及公告	符合	符合	
二、網路安全			
02.【網路控制措施】 (1)與外界連線，應僅限於經由教育局(處)網路管理單位之管控，以符合一致性與單一性之安全要求。 (2)宜依業務性質之不同，區分不同內部網路網段，例如：教學、行政、宿網等，以降低未經授權存取之風險。	不符合	符合	
03.【網路控制措施】 應禁止以私人架設網路（如：電話線、行動網路等）連結機房內之主機電腦或網路設備。 【無線網路存取】 應禁止使用者私自將無線網路存取設備介接至校園網路；若有介接之必要應經權責管理人員同意並設定帳號通行碼或加密金鑰以防未經許可之盜用。	符合	不符合	無「無線網路存取」相關規範
04.【網路控制措施】 對於開放提供外部使用者或廠商存取之服務，必須限制使用者之來源IP及網路連線埠(Port)，以確保安全。	符合	符合	
05.【無線網路存取】 校園內應提供無線網路存取服務，並採取適當安全管控措施： (1)專供行政使用之無線網路熱點建議設定加密金鑰防護，並避免使用開放之無線網路存取重要資訊系統及處理敏感性資料。	不適用	不符合	

06.(2)於教學區域、會議室等場所佈建之無線網路熱點應具有使用者身分認證機制，並經由校園無線路漫遊服務系統提供外校來賓使用。	符合	符合	
07.(3)專供師生教學活動使用之無線網路熱點，若採用其他管理方式確有不便時，應採取限定開放時間及限制開放區域等管理措施，減少遭受不當利用之機會。	不適用	不符合	
08.(4)開放校外人士出入之公共空間可視需要提供民眾無線上網服務，其網段應與校園網路隔離，或委由網路服務業者提供。	符合	不符合	
三、系統安全			
09.【設備區隔】 伺服器主機可依個別應用系統之需要，設置專屬主機，以避免未經授權之存取，例如網路服務主機(電子郵件、網站主機)、教學系統主機(例如隨選視訊主機)等。	符合	符合	
10.【對抗惡意軟體、隱密通道及特洛依木馬程式】 個人電腦應： (1)裝置防毒軟體，將軟體設定為自動定期更新病毒碼；或由伺服器端進行病毒碼更新的管理。 (2)作業系統及軟體應定期更新，以防範系統漏洞。	符合	符合	
11.【對抗惡意軟體、隱密通道及特洛依木馬程式】 個人電腦所使用的軟體應有授權。	符合	符合	
12.【對抗惡意軟體、隱密通道及特洛依木馬程式】 新伺服器系統啟用前，應執行相關程序(如：確認適合該作業系統之掃毒工具、預設通行碼更新、系統更新等，並記錄於啟用與報廢紀錄單)，以防範可能隱藏的病毒或後門程式。	符合	符合	
13.【桌面淨空與螢幕淨空政策】 個人辦公桌面應避免存放機敏性文件，結束工作時，應將其所經辦或使用具有機密	符合	符合	

或敏感特性的資料（如公文、學籍資料等）妥善存放。			
14.【桌面淨空與螢幕淨空政策】 當個人電腦或終端機不使用時，應使用鍵盤鎖或其他控管措施保護個人電腦及終端機安全，個人電腦應設定螢幕保護機制。	符合	符合	
15.【資料備份】 系統管理人員需針對學校重要電腦系統及資料（如:系統檔案、網站、資料庫等）應定期(建議每週至少進行一次)備份工作；建議使用設備執行異地備份或使用光碟、隨身碟或外接式硬碟執行異地存放。	符合	符合	
16.【資料備份】 每年應定期檢查備份資料之可用性與完整性。	符合	符合	
17.【資訊工作日誌】 系統管理人員需針對重要電腦系統進行檢查、維護、更新等動作時，應針對這些活動填寫日誌予以紀錄，作為未來需要時之查核。	符合	符合	
18.【資訊工作日誌】 系統管理人員應至少每季執行一次校時。	符合	符合	
19.【資訊存取限制】 共用的個人電腦（如：電腦教室電腦、教師休息室電腦等）應以特定功能為目的，並設定特定安全管控機制（如：限制從網路非法下載檔案行為、限制自行安裝軟體行為、限制特定資料的存取等）。	符合	符合	
20.【使用者註冊】 人員報到或離退職應會辦電腦系統帳號管理人員，執行電腦系統的使用者註冊及註銷程序，透過該註冊及註銷程序來控制使用者資訊服務的存取，該作業應包括以下內容： (1)使用唯一的使用者帳號。 (2)檢查使用者是否經過系統管理單位之授權使用資訊系統或服務。 (3)保存一份包含所有帳號註冊的記錄。 (4)使用者調職或離職後，應移除其帳號的存取權限。	符合	不符合	無「所有帳號註冊的記錄」

(5)每學期應檢查使用者帳號，以確保帳號的有效性。			
21.【特權管理】 電腦與網路系統資訊具有存取特權人員清單、及其所持有的權限說明，應予以文件化記錄。	符合	符合	
22.【通行碼（Password）之使用】 管制使用者第一次登入系統時，必須立即更改預設通行碼，預設通行碼應設定有效期限。	符合	符合	
23.【通行碼（Password）之使用】 資訊系統與服務應避免使用共用帳號及通行碼。	符合	符合	
24.【通行碼（Password）之使用】 由學校發佈通行碼制定與使用規則給使用者(參考優質通行碼設定原則與使用原則文件，文件編號：A-5)，內容應包含以下各項： 使用者應該對其個人所持有通行碼盡保密責任。 要求使用者的通行碼設定，應該包含英文字及數字，長度為8碼（含）以上。	符合	部分符合	無「通行碼設定規則之要求」
25.【通報安全事件與處理】 建立資訊安全事件（包括：任何來自網路的駭客攻擊、病毒感染、垃圾郵件、資料或網頁遭竄改、以及通訊中斷等）通報程序，通報程序包括學校內部通報，以及學校向教育機構通報平台通報。	符合	符合	
26.【通報安全事件與處理】 校內人員應了解通報的管道，並將資訊安全事件通報程序應公布於校園內使用電腦與網路之場所，提供使用者了解。	符合	符合	
四、實體安全			
27.【設備安置及保護】 主機機房及電腦教室宜設置偵煙、偵熱或滅火設備（氣體式滅火器），並禁止擺放易燃物或飲食。	部分符合	部分符合	宜設置滅火設備
28.【設備安置及保護】	符合	符合	

主機機房及電腦教室的電源線插頭應有接地的連結或有避雷針 等裝置，避免如雷擊事件所造成損害情況。			
29.【設備安置及保護】 主機機房及電腦教室應實施門禁管制。	符合	符合	
30.【溫濕度控制】 重要的資訊設備（如：主機機房等）宜有溫濕度控制措施(溫度建議控制在 20℃~25℃，濕度建議控制在相對濕度 50%R.H.~70%R.H.)，以防止資訊設備意外損壞。機房內應有溫濕度顯示裝置，以觀察實際之溫濕度情況。	符合	不符合	有設備但無顯示溫濕度相關資訊
31.【電源供應】 重要的資訊設備（如主機機房）應有適當的電力保護設施，例如設置UPS、電源保護措施(如穩壓器、接地等)，以免斷電或過負載而造成損失，並設置緊急照明設備以作為停電照明之用。	符合	部分符合	無緊急照明設備
32.【纜線安全】 主機機房及電腦教室內線路應考量設置保護設施(如：高架地板、線槽、套管等)。	符合	符合	
33.【設備與儲存媒體之安全報廢或再使用】 所有包括儲存媒體的設備項目，在報廢前應填寫「啟用與報廢紀錄單」，確認已將任何敏感資料和授權軟體刪除或覆寫。	符合	符合	
34.【財產攜出】 禁止資訊設備在未經授權之情況下攜離所屬區域，若需將設備攜出，應遵守財產管理相關規定並填寫「設備進出紀錄表」。	符合	符合	
35.【財產攜出】 當有必要將設備移出，應檢視相關授權，並實施登記與歸還記錄。	符合	符合	
五、可攜式電腦設備與媒體			
36.公務用可攜式電腦設備(如：筆記型電腦、平板電腦、智慧型手機等)應設定保護機制，如設定通行碼、圖形辨識、臉孔	符合	符合	

辨識或指紋辨識等。 公務用可攜式電腦設備應執行安全相關程序(如：掃毒、預設通行碼更新、系統更新等)，以防範可能隱藏的病毒或後門程式。			
37.公務用可攜式儲存媒體(如：隨身碟、光碟、磁帶等)應依儲存資料的機敏性實施安全控管措施，如檔案加密儲存或將該儲存媒體存放於上鎖儲櫃或安全處所。	符合	符合	
六、人員安全			
38.【人員安全責任】 非正式人員、約聘(僱)人員者，因業務需要，而接觸公務機密、個人權益及學校機敏資料者須填寫保密切結書。	符合	符合	
39.【資訊安全教育與訓練】 鼓勵資安業務承辦人參加資安管理系統相關教育訓練。	符合	符合	
40.【資訊安全教育與訓練】 鼓勵所有教職員參與資訊安全教育訓練或宣導活動，以提昇資訊安全認知。	符合	符合	
七、資訊業務委外管理			
41.【服務委外廠商合約之安全要求】 在資訊業務委外合約中，應訂定委外廠商的資訊安全責任及保密規定。	不適用	不適用	
42.【服務委外廠商合約之安全要求】 應要求委外廠商簽訂安全保密切結書。	不適用	不適用	
43.委外廠商人員到校服務時，應請其簽署委外廠商人員保密切結書。	不適用	不適用	
44.委外廠商服務異動或終止時，應中止或刪除其系統上的帳號與權限。	不適用	不適用	
八、法令認知			
45.宣導師生遵守智慧財產權、個人資料保護法及其施行細則、刑法電腦犯罪專章等相關法令規定。	符合	符合	

九、個人資料保護法			
46.【規劃】 建立個人資料保護管理政策。	未填	不符合	
47.【界定個人資料之範圍】 進行個人資料盤點後，建立「個人資料檔案清冊」，並依個資法規定於網站公布個人資料檔案大綱。	未填	不符合	
48.【個人資料蒐集、處理及利用之內部管理程序】 進行個人資料之蒐集與利用時，必須符合法令規定，包含： (1)個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。 (2)蒐集個人資料時，應依法令規定告知當事人蒐集資料之目的、利用範圍等資訊。 (3)除符合法令規定外，有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用(當事人如書面同意即可蒐集)。 (4)當資料利用範圍超出蒐集的特定目的時，應依個資法規定取得當事人之書面同意。	未填	不符合	
49.【事故之預防、通報及應變機制】 學校須設置「個資保護聯絡窗口」，協調聯繫個資事宜，並將聯繫方式(如：電話、email)置於單位網站，以便利民眾提出申訴與救濟。	未填	不符合	
50.【資料安全管理】 對於個人資料之調閱，須有申請及核准程序，並記錄保存調閱者身分及行為。	未填	不符合	