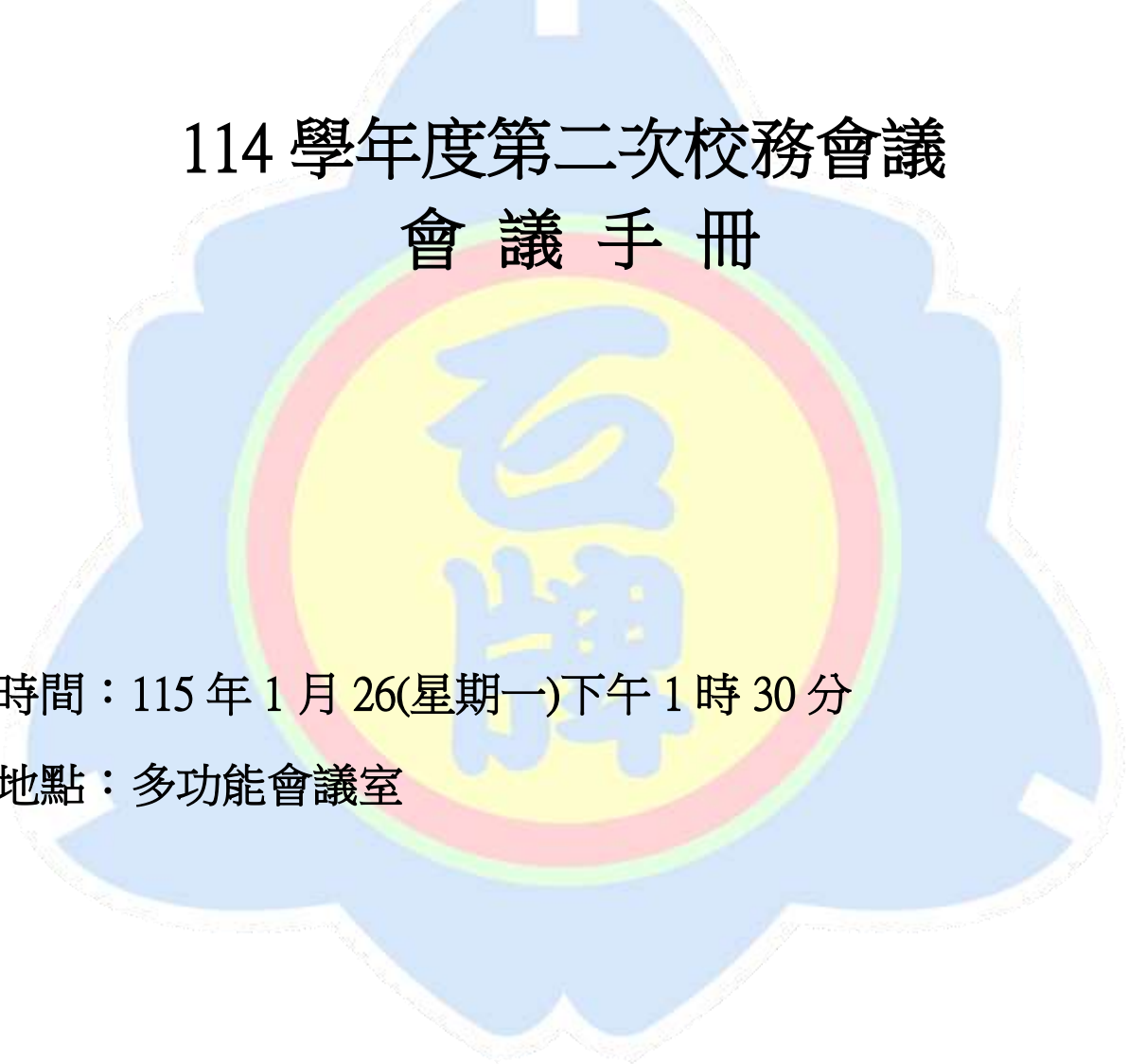


臺北市北投區石牌國民小學

114 學年度第二次校務會議
會議手冊

開會時間：115 年 1 月 26(星期一)下午 1 時 30 分

開會地點：多功能會議室



目 次

壹、會議程序.....	P3
貳、報告事項.....	P3
(一)報告上次會議決議案執行情形	
【提案一】修正本校專任教師聘約一案.....	P3
【提案二】修正本校代理教師聘約一案.....	P3
【提案三】修訂本校學生成績評量辦法.....	P3
參、校務會議提案.....	P5
【提案一】115 年度臺北市北投區石牌國民小學資訊安全 維護計畫，敬請討論.....	P5
【提案二】修正本校性騷擾防治措施、申訴及懲戒規範一案。.....	P6
肆、上次會議決議案執行情形之附件.....	P8
附件一 修正本校專任教師聘約一案執行情形 :臺北市北投區石牌 國民小學教師聘約.....	P8
附件二 修正本校代理教師聘約一案執行情形 臺北市北投區石牌國民小學 代理教師聘約.....	P12
伍、校務會議提案附件.....	P14
附件三 115 年度臺北市北投區石牌國民小學資訊安全維護計畫附件...	P14
附件四 修正本校性騷擾防治措施、申訴及懲戒規範一案附件.....	P92

壹、會議程序

- 一、主席主持開議
 確定出席人數及議程
- 二、報告事項
 - (一)、報告上次會議決議案執行情形
 - (二)、各委員會報告。(若無從略)
- 三、提案討論
- 四、臨時動議
- 五、建議事項
- 六、散會

貳、報告事項

(一)、上次會議決議情形報告:

【提案一】修正「修正本校專任教師聘約」一案。

【提案人】人事室

【上次決議情形】逕付表決。同意 29 票 不同意 0 票 本案由主席宣布「通過」。

【執行情形】依會議決議辦理修正專任教師聘約。詳如附件一

【提案二】修正「本校代理教師聘約」一案。。

【提案人】人事室

【上次決議情形】逕付表決。同意 29 票 不同意 0 票 本案由主席宣布「通過」

【執行情形】依會議決議辦理修正代理教師聘約。詳如附件二

【提案三】修訂本校學生成績評量辦法

【提案人】教務處

【上次決議情形】 逕付表決。同意 29 票 不同意 0 票 本案由主席宣布「通過」

【執行情形】 已於 114 學年度第一次期中評量執行，未接獲相關反應事項。

修正臺北市北投區石牌國民小學學生成績評量辦法

修正條文	現行條文	說明	實施現況
標題：臺北市北投區石牌國民小學學生定期評量紙筆測驗注意事項	標題：臺北市北投區石牌國民小學學生成績評量辦法	一、依照教育局最新函文修正本校辦法。	依修正條文實施，符合教育局規範。
一、臺北市北投區石牌國民小學(以下簡稱本校)依「臺北市國民小學及國民中學學生成績評量補充規定」第五條第一款，訂定本作業規定。	一、臺北市北投區石牌國民小學(以下簡稱本校)依「臺北市國民小學及國民中學學生成績評量補充規定」(中華民國108年11月5日臺北市政府教育局(108)北市教國字第1083108062號函修正)第三條，訂定本作業規定。	一、依照教育局最新函文修正本校辦法。	依修正條文實施，符合教育局規範。
三、本校訂定之作業流程，包含命題、繳交試題、審閱、印製、發卷、收卷、閱卷、成績統計及分數應用與補救教學之實施等項目。	三、本校訂定之作業流程，包含命題、繳交試題、審閱、印製、發卷、收卷、閱卷、成績統計及分數應用與補救教學之實施等項目(如附件:本校學生定期評量紙筆測驗作業流程及說明)。	一、依照教育局最新函文修正本校辦法。	依修正條文實施，符合教育局規範。
四、本校教師應秉持專業，依據教學計畫之進度範圍設計評量試題，命題內容應兼顧記憶、了解、應用、分析、評鑑、創造等層面。	四、本校教師應秉持專業，依據教學計畫之進度範圍設計評量試題，命題內容應兼顧知識、理解、應用、分析、綜合、評鑑等層面。	一、依照教育局最新函文修正本校辦法。	依修正條文實施，符合教育局規範。

六、本校得對各班平時評量之作業流程及評量內容進行不定期稽查。	無	一、依照教育局最新函文修正本校辦法。 二、因新增第六項，第七、八、九、十、十一點次變更。	依修正條文實施，符合教育局規範。
十一、本注意事項規定提校務會議通過，經校長核可後實施，修正時亦同。	十一、本作業規定提校務會議通過，經校長核可後實施，修正時亦同。	一、依照教育局最新函文修正本校辦法。	依修正條文實施，符合教育局規範。
備註:2 學校教育人員不得有洩題或暴露試卷之行為，違者依相關規定懲處。	備註:2. 不得將試卷影印或外流，亦不得以任何形式洩露給他人。	一、依照教育局最新函文修正本校辦法。	依修正條文實施，符合教育局規範。

(二)、各委員會報告。(若無從略)

參、校務會議提案

【提案一】115 年度臺北市北投區石牌國民小學資訊安全維護計畫，敬請討論

【提案人】 教務處

提案日期：114 年 12 月 23 日

提案人	教務主任鐘民儒
連署人	
提案類別	<input type="checkbox"/> 校長交議。 <input checked="" type="checkbox"/> 相關之處室主任提案。 <input type="checkbox"/> 家長會或教師會提案。 <input type="checkbox"/> 教職員工及家長，經校務會議成員四分之一以上連署之提案。

案 由	115 年度臺北市北投區石牌國民小學資訊安全維護計畫，敬請討論
說 明	1. 根據 111 年 7 月 13 日臺北市政府資通安全管理規定辦理。 2. 根據 113 年 4 月 17 日北市教資字第 1133051191 號函，各校應於每年度行政院國家資通安全會報資通安全作業管考系統(https://s.moda.gov.tw/L1uZY6huneta)進行資通安全填報作業。
辦 法	校務會議通過後即日起頒行實施。

詳如附件三：115 年度臺北市北投區石牌國民小學資訊安全維護計畫

【提案二】修正本校性騷擾防治措施、申訴及懲戒規範一案。

【提案人】 人事室

提案日期：115 年 1 月 2 日

提案人	人事室
連署人	
提案類別	<input type="checkbox"/> 校長交議。 <input checked="" type="checkbox"/> 相關之處室主任提案。 <input type="checkbox"/> 家長會或教師會提案。 <input type="checkbox"/> 教職員工及家長，經校務會議成員四分之一以上連署之提案。

案 由	修正本校性騷擾防治措施、申訴及懲戒規範一案。
說 明	<p>一、依臺北市政府教育局 114 年 11 月 7 日北市教人字第 1143112221 號函略以，各級學校依據性騷擾防治法第 7 條及性別平等工作法第 13 條訂定性騷擾防治措施（包含三法整合之處理機制）等校內章則，均屬校務重大事項，應提交校務會議議決。</p> <p>二、修正第 24 條程序，並酌作文字修正。</p>
辦 法	臺北市政府教育局 114 年 11 月 7 日北市教人字第 1143112221 號函

詳如附件四：臺北市北投區石牌國民小學性騷擾防治措施、申訴及懲戒規範修正條文對照表；臺北市北投區石牌國民小學性騷擾防、申訴及懲戒規範修正草案；臺北市政府教育局函

肆、上次會議決議執行之附件

附件一 修正本校教師聘約一案執行情形之附件： 臺北市北投區石牌國民小學 教師聘約

中華民國 114 年 8 月 28 日校務會議修正

臺北市北投區石牌國民小學(以下簡稱甲方)敦聘 君(以下簡稱乙方)為本校專任教師，茲就甲、乙雙方權利與義務事宜，訂定本聘約。

第一章 總則

第一條 本聘約依據臺北市高級中等以下學校教師聘約準則暫行要點訂定之。

第二條 本聘約為本校與編制內專任教師間之唯一聘約，全校編制內專任教師一體適用。

甲、乙雙方不得與任何個人或團體另定本校聘約，否則視同重大違約，若因而造成他方傷害或損失者，得依法請求賠償。

第二章 聘期

第三條 乙方之聘期：

初聘：自中華民國 年 月 日起至中華民國 年 月 日止。

續聘：自中華民國 年 月 日起至中華民國 年 月 日止。

長期聘任：自中華民國 年 月 日起至中華民國 年 月 日止。

第四條 新聘教師接到聘書後，應於甲方規定期限內將應聘書送交甲方，逾期仍未應聘者，甲方以卻聘論，甲方並於七日內通知乙方。

第五條 乙方新聘到校時，甲方應即告知乙方洽填各種表件，填妥後連同所需證件，辦理陳報核薪手續（續聘者不在此限），如因證件經審核不合格，應即通知其補件，若仍無法通過而延誤核薪者，甲方概不負責。若因甲方延誤而造成乙方損失時，甲方應補足乙方應得之薪資。

第六條 乙方新聘到校時，若因乙方不符聘任資格或未能於起聘日前到校報到者，本聘約無效，甲方概不負責。

第三章 工作要求與工作條件

第七條 乙方接受聘任後，依有關法令及學校章則之規定，享有下列權利：

一、對學校教學及行政事項提供興革意見。

二、享有待遇、福利、退休、撫卹、資遣、保險等權益及保障。

三、參加在職進修、研究及學術交流活動。

四、參加教師組織，並參與其他依法令規定所舉辦之活動。

五、對主管教育行政機關或學校有關其個人之措施，認為違法或不當致損害其權益者，得依法提出申訴。

六、教師之教學及對學生之輔導依法令及學校章則享有專業自主。

七、除法令另有規定者外，教師得拒絕參與教育行政機關或學校所指派與教學無關之工作或活動。

八、其他依教師法或其他法律應享之權利。

- 第八條 乙方除應遵守法令履行聘約外，並負有下列義務：
- 一、遵守聘約規定，維護校譽。
 - 二、積極維護學生受教之權益。
 - 三、依有關法令及學校安排之課程，實施教學活動。
 - 四、輔導或管教學生，導引其適性發展，並培養其健全人格。
 - 五、從事與教學有關之研究、進修。
 - 六、嚴守職分，本於良知，發揚師道及專業精神。
 - 七、依有關法令參與學校學術、行政工作及社會教育活動。
 - 八、非依法律規定不得洩漏學生個人或其家庭資料。
 - 九、其他依教師法或其他法律規定應盡之義務。
- 第九條 寒、暑假期間乙方應有從事研究、進修、編選教材之權利與義務。
- 第十條 乙方之權利、義務、待遇、進修與研究、退休、撫卹、離職、資遣、保險、申訴及訴訟等均依教師法及相關法令規定辦理，法令未規定者依本聘約。
- 第十一條 乙方應自編或自選教材。乙方對於教材、教法及教學活動實施方式，應本專業自主原則進行。乙方依專業知能有決定評量方式之權利。
- 第十二條 乙方執行職務致損害他人權益時，悉依國家賠償法相關規定辦理。
- 第十三條 乙方之上課、上班、差假及相關規定，依臺北市政府教育局與本市教師會邀請教師代表、家長代表及相關單位代表等研商訂定之基本原則辦理。在未訂定前暫依現行規定辦理。
- 第十四條 乙方之授課科目應依課程標準，以專業專才及公平原則妥適編排。授課時數由甲方與本校教師會根據員額編制（含專、兼任、代理代課教師、行政人員及特殊班之相關專業人員），制定編配原則，經校務會議決議後施行之，修改時亦同。乙方兼任教師會及本職以外與教育有關之其他職務時得酌減其授課時數，或給與一定時間之公假，其標準由甲方與本校教師會協商議定之。
- 第十五條 甲方得聘乙方擔任班級導師、實習輔導教師及兼任行政工作，但前述人員產生困難時，由校長與本校教師會共同制定延聘規則，受聘教師均應遵守。
- 第十六條 乙方獲長期聘任者，應由政府視財政狀況給予進修、研究等之補助，並每七年給予一學期之進修權利。
- 第十七條 甲方應將教師進修研究機會與資訊公開，並依公平原則給與乙方進修機會。
- 第十八條 甲方應依公平妥適之原則提供場地給教師舉辦親師活動、校內教師聯誼及教育有關之各項活動。並依現有空間及設施以公平原則提供乙方上課教室、辦公室及其設備、休息室、教具、教學設備及其他教學資源。
- 第十九條 乙方應與學生家長就學生教育各項事宜相互溝通，但應事先約定雙方同意之時間及地點，如有必要須由甲方出面與家長協商之。為避免學生生命、身體、自由及財產上急迫之危險或其他緊急事由，乙方需立即處理時，不在此限。
- 第二十條 乙方應本教育專業原則就學生特質及教材斟酌教學及評量之實施方式，並不斷檢討改進追求專業成長。
- 前述之實施方式遇有學生監護人提出書面質疑時，交由本校教師評審委員會邀請相關專業人士研商解決。
- 各主管教育行政機關若接獲學生監護人前項之投訴，亦應先交依前項程序辦理。
- 甲方行政單位應配合乙方教學上之正當要求。所謂正當要求指：與行政部門共同使用器材、消耗品、場地及人力資源，及對學校採購物品種類、規格之建議。
- 乙方應接受主管教育行政機關基於提昇教學品質所進行之教學專業視導與評鑑。
- 第二十一條 甲方因減班、停辦、解散時，乙方為裁減人員之列，甲方應先預告乙方並依教師法第十一條規定辦理，按公平原則妥適安排。如有爭議則由本校教師評審委員會制定原則。
- 第二十二條 乙方基於教育需要及維護多數學生之受教權益，甲方應邀請本校教師會及家長會代表共同研議管教規範與實施方式，經校務會議決議後施行。
- 第二十三條 本校班級導師的工作內容，甲方應與本校教師會協商另訂之。

第廿四條 本校附設幼兒園之專任教師對協助園務行政工作之分配、任教班級之編排，甲方得聘任之。如編配發生困難時，應召開園務會議訂定規則共同遵守。

第廿五條 乙方於執行教學、指導、訓練、評鑑、管理、輔導或提供學生工作機會時，在與性或性別有關之人際互動上，不得發展有違專業倫理之關係。

乙方發現師生關係有違反前項專業倫理之虞，應主動迴避或陳報甲方處理。

第廿六條 乙方應尊重他人與自己之性或身體之自主，避免不受歡迎之追求行為，並不得以強制或暴力手段處理與性或性別有關之衝突。

第廿七條 甲乙雙方應遵守校園霸凌防治準則之相關規定。

第四章 履約與違約罰則

第廿八條 乙方接受聘任後，甲方非依教師法第十三條有關規定，不得解聘、停聘或不續聘。

第廿九條 聘約期限未到，乙方如有不得已之情形必須中止或解除聘約，應依本校教師評審委員會設置及評審作業要點第廿七條規定提出申請經甲方同意後，始得為之。惟如有屆齡退休，自願退休及其他正當理由者，甲方應予同意。

第三十條 乙方違約之認定，由本校教師評審委員會依聘約及相關法令規定審議之。

除聘約及法令另有規定者外，其餘依下列原則辦理之：

輕微違約：以口頭通知改善。

一般違約：以書面通知改善。

連續違約：再次書面通知。

嚴重違約：依相關法令辦理。

第三十一條 聘約有效期間，乙方未經甲方同意，中途離職、中止或解除聘約時，視同違約。

乙方應賠償違約日至甲方新聘任教師聘約生效前支付之代課費，但以三個月為限。

第三十二條 甲方違反聘約，乙方得依教師法第七章之規定尋求救濟或提起訴訟。

第三十三條 因甲方之過失致乙方喪失工作權，乙方得請求回復原聘及賠償其所造成之損失。

乙方執行職務之安全，甲方應予保障，對於乙方之執行職務，應提供安全及衛生之防護措施。

甲方未依相關法令規定，致乙方受到傷害者，乙方得請求賠償其所造成之損失。

乙方之長官或主管不得作違法之工作指派，亦不得以強暴脅迫或其他不正當方法，使乙方為非法之行為。

乙方依法執行職務涉訟或遭受侵害時，甲方有義務維護乙方權益，應延聘律師為其辯護及提供法律上之協助。

乙方依本條之請求權按公務人員保障法相關規定辦理。

第五章 聘約修改與訴訟管轄法院

第三十四條 甲、乙雙方同意本校教師聘約之制定與修改，由甲方與本校教師會協議訂定。協議雙方有爭議時，應由雙方、臺北市教師會及臺北市政府教育局協商解決之。

第三十五條 本聘約於有效期間內修改，甲方應於十日內書面通知乙方，乙方得重新簽訂聘約，其聘期與原約同，惟對前述修改聘約之承諾應於三十日內為之，逾期不重新簽訂聘約或不為承諾時，視同不受聘。

第三十六條 聘約存續期間，甲、乙雙方就權利義務關係之新生調整事項，應由校長與本校教師會協商後訂定之。

第三十七條 教師法及相關法令修正時，甲、乙雙方同意由校長與本校教師會協商後隨同修正本聘約，並加載於聘約中。

第三十八條 甲、乙雙方因聘約所生之訴訟，以本校所在地之法院為第一審管轄法院。

第六章 附則

第三十九條 本聘約內容如有未盡事宜，依教師法及相關法令規定辦理。

第四十條 本聘約一式兩份，甲、乙雙方各執一份，自應聘之日起生效。

附錄：教育部「學校校長及教職員工違反與性或性別有關之專業倫理防治指引」。(本校校網首頁/行政組織/人事室/本校教職員工聘約附錄)

立 約 人

甲 方：臺北市北投區石牌
國民小學

法定代理人：
(蓋章)

地 址：臺北市北投區致遠
二路 80 號

電 話：(0 2) 2 8 2 2 7
4 8 4

立 約 人

乙 方：
(簽章)

身分證字號：

地 址：

電 話：

中 華 民 國 年 月 日

附件二 修正本校代理教師約一案執行情形之附件：臺北市北投區石牌國民小學代理教師聘約

中華民國 114 年 8 月 28 日校務會議修正

臺北市北投區石牌國民小學(以下簡稱甲方)應業務需要，敦聘_____教師(以下簡稱乙方)為本校代理(課)教師。雙方基於自由意志，同意下列條款：

第一條：立約依據

- 一、本聘約參照教師法及其施行細則、臺北市高級中等以下學校教師聘約準則暫行要點及相關法令訂定。
- 二、代理教師之授課、聘期、終止聘約、停止聘約執行、待遇、請假、保險、退休金及其他相關權利義務等均依「高級中等以下學校兼任代課及代理教師聘任辦法」及相關法令規定辦理。
- 三、代理教師之給假依「行政院與所屬中央及地方各機關聘僱人員給假辦法」及「臺北市立各級學校教師請假作業補充規定」辦理。

第二條：代理期間及限制

- 一、代理期間：自中華民國_____年_____月_____日起至_____年_____月_____日止。
- 二、接聘之乙方不得再至他校應聘，如有違背將視同不良紀錄，5 年內不得再到本校應徵任何職務。

第三條：聘約終止

- 一、在聘約有效期間內，乙方若有正當理由，經甲方同意，得申請辭聘。
- 二、在聘約有效期間內，乙方如有另求他職之意，應在離職日前 1 個月以書面告知甲方，經甲方同意並完成工作交接後，始可辦理離職手續。
- 三、未於應(回)聘截止日前接聘之乙方，視同不接聘，甲方得依法選(遴)聘其他教師。若有不可抗拒之事由者不在此限。
- 四、乙方新聘到校時，若乙方未能於起聘日前完成報到手續，則本契約無效，乙方因而喪失受聘資格，甲方概不負責。
- 五、乙方於代理原因消失時，應即解除代理，不得以任何理由要求留用或救助。

第四條：工作條件

- 一、甲方應依現行相關法令規定，按月給付乙方工作薪給。經公開甄選聘任 3 個月以上代理教師，惟實際代理期間未滿 3 個月即離職之薪資支給方式，依聘約所定聘期認定。
- 二、乙方應依約戮力積極執行公務，若遭受暴力、脅迫時，甲方得會同本校教師會、家長會協助排除危難。
- 三、乙方為專任職，不得在外補習，違法兼職兼課，或藉職務之便從事私人商業行為，或未經甲方同意請他人擔任職務。

第五條：工作要求

- 一、乙方差假，依現行規定辦理。如法令有修正或廢止時，依新修正或新制訂之法令辦理。
- 二、乙方應遵守教師自律公約。
- 三、校長得聘乙方擔任班級導師、科任教師及兼任行政工作或其他專案工作，受聘之乙方教師應遵守。
- 四、乙方應接受甲方及主管教育行政機關基於提昇教學品質所進行之教學專業視導及評鑑。
- 五、寒、暑假期間因應有關教學及行政上之公務需要，乙方應到校承擔工作，不得任意請假。
- 六、乙方有配合學校各項與教學及行政相關活動之義務。
- 七、乙方應指導學生參加所任教科目之校內外比賽及活動。
- 八、甲乙雙方應遵守校園霸凌防治準則、校園性侵害性騷擾或性霸凌防治準則之相關規定。

第六條：違約罰則

- 一、乙方若違反聘約，甲方得依乙方違反聘約情節，經甲方召開教師評審委員會之決議，為解聘、停聘、不續聘之處分，或依人事法規作適當之處置。
- 二、乙方若未經第三條第 1 款、第 2 款之程序，任意中途離職、終止或解約時，視同毀約，甲方得依法追究並要求賠償之。

第七條：申訴程序

- 一、乙方之教材教法、教學活動及評量實施方式等應接受甲方之指導，遇有受教學生之家長或監護人提出書面質疑時，乙方應妥當提出說明；再有爭議時，交由教師評審委員會邀請相關專業人士研商解決。
- 二、甲方若接獲學生家長或監護人前項之投(申)訴，在維護教師專業及尊嚴的原則下得先行處理，必要時得予乙方解釋說明之機會。

第八條：訴訟管轄法院

因本聘約所生之訴訟，其第一審由臺灣士林地方法院受理之。

附錄：教育部「學校校長及教職員工違反與性或性別有關之專業倫理防治指引」。(本校校網首頁/行政組織/人事室/本校教職員工聘約附錄)

本聘約一式 2 份，甲、乙雙方各執乙份為憑，自應聘之日起生效。

立約人

甲 方：臺北市北投區石牌國民小學

法定代理人： (蓋章)

地 址：臺北市北投區致遠二路 80 號

立約人

乙 方： (簽章)

身份證字號：

地 址：

中華民國 年 月 日

伍、校務會議提案附件

附件三

臺北市北投區石牌國民小學 資訊安全維護計畫(稿)

第8.0版

生效日期：115年1月26日

目次

壹、資通安全推動小組成員及分工表	4
貳、實施計畫.....	5
一、依據及目的.....	5
二、適用範圍	5
三、核心業務及重要性.....	5
四、資通安全政策及目標	7
五、資通安全推動組織.....	8
六、專職人力及經費配置	10
七、資訊及資通系統之盤點	12
八、資通安全風險評估.....	14
九、資通安全防護及控制措施	14
十、資通安全事件通報、應變及演練相關機制	23
十一、資通安全情資之評估及因應	23
十二、資通系統或服務委外辦理之管理	25
十三、資通安全教育訓練.....	26
十四、公務機關所屬人員辦理業務涉及資通安全事項之考核機制.....	27
十五、資通安全維護計畫及實施情形之持續精進及績效管理機制.....	27
十六、資通安全維護計畫實施情形之提出.....	30
十七、相關法規、程序及表單.....	30

壹、資通安全推動小組成員及分工表

臺北市北投區石牌國民小學資通安全推動小組成員及分工表

單位職級	組別	職掌事項	分機	代理人
校長	策略規劃組	1. 學校資訊安全推動小組召集人 2. 統籌及督導資訊安全業務 3. 學校資訊安全推動小組資安長	188	教務主任
教務主任	績效管理組	1. 推動全校資訊安全工作相關業務 2. 資訊安全第一聯絡人	111	教學組長
學務主任		督導學生事務相關資訊安全工作	221	生教組長
總務主任		1. 支援校園資訊安全相關庶務工作 2. 經費請購與設備採買事宜	331	事務組長
輔導主任		督導學生輔導相關資訊安全工作	551	輔導組長
幼兒園主任		督導幼兒園相關資訊安全工作	170	幼兒園 教學組長
人事主任		辦理資通安全內部稽核工作	661	人事書記
會計主任		資訊安全工作相關經費核銷事宜	663	會計佐理員
資訊小組 學年代表		1. 協助溝通傳達校園資訊安全工作事宜	無	各學年教師
資訊組長		資安管理組	1. 資訊安全第二聯絡人 2. 資安事件通報與處理 3. 校園網路安全工作 4. 防火牆管理及網路流量監控 5. 行政及教學電腦防毒防駭 6. 校內電腦作業系統及病毒碼定期更新 7. 辦理教師及學生資訊安全、相關法令之研習宣導 8. 其他相關資訊安全業務	115

系統管理師	<ol style="list-style-type: none">1. 資通安全事件通報2. 資訊設備維作運護	115	資訊組長
-------	---	-----	------

貳、 實施計畫

一、 依據及目的：

本計畫依據資通安全管理法第 10 條及施行細則第 6 條訂定。

本計畫依據下列法規訂定：

- (一) 資通安全管理法第 10 條及其施行細則第 6 條。
- (二) 其他業務法規名稱。

二、 適用範圍：

本計畫適用範圍涵蓋本機關。

三、 核心業務及重要性

(一) 核心業務及重要性：

本機關之核心業務及重要性如下表：

核心業務	核心資通系統	重要性說明	業務失效影響說明	最大可容忍中斷時間
教務	(略)	為本機關依組織法執掌，足認為重要者	無	無
學務	(略)	為本機關依組織法執掌，足認為重要者	無	無
總務	(略)	為本機關依組織法執掌，足認為重要者	無	無
輔導	(略)	為本機關依組織法執掌，足認為重要者	無	無

各欄位定義：

1. 核心業務名稱：請參考資通安全管理法施行細則第 7 條之規定列示。
2. 作業名稱：該項業務內各項作業程序的名稱。
3. 重要性說明：說明該業務對機關之重要性，例如對機關財務及信譽上影

響，對民眾影響，對社會經濟影響，對其他機關業務運作影響，
法律遵循性影響或其他重要性之說明。

1. 最大可容忍中斷時間單位以小時計。

(二) 非核心業務及說明：

本機關之非核心業務及說明如下表：

非核心業務	業務失效影響說明	最大可容忍中斷時間
(略)	(略)	(略)
(略)	(略)	(略)
(略)	(略)	(略)
(略)	(略)	(略)
(略)	(略)	(略)
(略)	(略)	(略)
(略)	(略)	(略)
(略)	(略)	(略)
其他：非屬上開業務範疇及 核心業務者	影響機關行政效率	24 小時

各欄位定義：

1. 業務名稱：公務機關之非核心業務至少應包含輔助單位之業務名稱，

如差勤服務、郵件服務、用戶端服務等。

2. 作業名稱：該項業務內各項作業程序的名稱。
3. 說明：說明該業務之內容。
4. 最大可容忍中斷時間單位以小計。

四、資通安全政策及目標

(一) 資通安全政策

為使本機關業務順利運作，防止資訊或資通業務受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性(Confidentiality)、完整性(Integrity)及可用性(Availability)，特制訂本政策如下，以供全體同仁共同遵循：

1. 定期因應內外資通安全情勢變化，檢討資通安全風險管理之有效性。
2. 針對各資料的機密性與完整性應妥善保護，避免資料遭竄改。
3. 建立資通安全防護（如：防火牆、防毒軟體）
4. 辦理資通安全教育訓練，提升同仁資通安全意識。
5. 針對辦理資通安全業務有功相關人員，應依資通安全管理法子法之

「公務機關所屬人員資通安全事項獎懲辦法」進行獎勵。

6. 禁止多人共用同一帳號。
7. 落實資通安全通報機制。

(二) 資通安全目標

1. 資安事件發生，於規定的時間完成通報、應變及復原作業。
2. 全年度資安通報平臺之資安事件等級第 1、2 級發生件數少於 3 件

(含) 以下，等級第 3、4 級不得發生。

1. 達成資通安全責任等級分級之要求，並降低遭受資通安全風險之威脅。

(三) 資通安全政策及目標核定程序

資通安全政策由本機關資訊組簽陳至資通安全長，由校務會議通過實施。

(四) 資通安全政策及目標之宣導

1. 本機關之資通安全政策及目標應每年透過教育訓練、內部會議、張貼公告等方式，向機關內所有人員進行宣導，並檢視執行成效。
2. 本機關應每年向利害關係人（例如：社團報名系統委由廠商建置）進行資安政策及目標宣導，並檢視執行成效。

(五) 資通安全政策及目標定期檢討程序

資通安全政策及目標，應定期於學校資訊小組會議中檢討其適切性。

五、資通安全推動組織

(一) 資通安全長

依本法第 11 條之規定，本機關訂定校長為資通安全長，負責督導機關資通安全相關事項，其任務包括：

1. 資通安全管理政策及目標之核定、核轉及督導。
2. 資通安全責任之分配及協調。
3. 資通安全資源分配。
4. 資通安全防護措施之監督。
5. 資通安全事件之檢討及監督。

1. 資通安全相關規章與程序、制度文件核定。
2. 資通安全管理年度工作計畫之核定。
3. 資通安全相關工作事項督導及績效管理。
4. 其他資通安全事項之核定。

(二) 資通安全推動小組

1. 組織

為推動本機關之資通安全相關政策、落實資通安全事件通報及相關應變處理，由資通安全長召集各學年上之教師代表成立資通安全推動小組，其任務包括：

- (1) 跨處室資通安全事項權責分工之協調。
- (2) 應採用之資通安全技術、方法及程序之協調研議。
- (3) 整體資通安全措施之協調研議。
- (4) 資通安全計畫之協調研議。
- (5) 其他重要資通安全事項之協調研議。

2. 分工及職掌

本機關之資通安全推動小組依下列分工進行責任分組，並依資通安全長之指示負責下列事項，本機關資通安全推動小組分組人員名單及職掌應列冊，並適時更新之：

- (1) 策略規劃組：
 - i. 資通安全政策及目標之研議。

- i. 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。
- ii. 依據資通安全目標擬定機關年度工作計畫。
- iii. 傳達機關資通安全政策與目標。
- iv. 其他資通安全事項之規劃。

(2) 資安防護組：

- i. 資通安全技術之研究、建置及評估相關事項。
- ii. 資通安全相關規章與程序、制度之執行。
- iii. 資訊及資通系統之盤點及風險評估。
- iv. 資料及資通系統之安全防護事項之執行。
- v. 資通安全事件之通報及應變機制之執行。
- vi. 其他資通安全事項之辦理與推動。

(3) 績效管理組：

- i. 辦理資通安全內部稽核。
- ii. 每年 10 月前召開資通安全管理審查會議，提報資通安全事項執行情

- i. 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。
- ii. 依據資通安全目標擬定機關年度工作計畫。
- iii. 傳達機關資通安全政策與目標。
- iv. 其他資通安全事項之規劃。

(2) 資安防護組：

- i. 資通安全技術之研究、建置及評估相關事項。
- ii. 資通安全相關規章與程序、制度之執行。
- iii. 資訊及資通系統之盤點及風險評估。
- iv. 資料及資通系統之安全防護事項之執行。
- v. 資通安全事件之通報及應變機制之執行。
- vi. 其他資通安全事項之辦理與推動。

(3) 績效管理組：

- i. 辦理資通安全內部稽核。
- ii. 每年 10 月前召開資通安全管理審查會議，提報資通安全事項執行情

級，最低應設置資通安全兼辦人員 1 人，其分工如下，本機關現有資通安全專責人員名單及職掌應列冊，並適時更新。

- (1) 負責資通系統分級、內部資通安全稽核、防護基準及教育訓練業務之推動。
 - (2) 負責資通安全防護設施建置及資通安全事件通報及應變業務之推動。
2. 本機關之承辦單位於辦理資通安全人力資源業務時，應加強資通安全人員之培訓，並提升機關內資通安全專業人員之資通安全管理能力。本機關之相關單位於辦理資通安全業務時，如資通安全人力或經驗不足，得洽請相關學者專家或專業機關（構）提供顧問諮詢服務。
 3. 本機關負責重要資通設備之管理、維護、設計及操作之人員，應妥適分工，分散權責，若負有機密維護責任者，應簽屬書面約定，並視需要實施人員輪調，建立人力備援制度。
 4. 本機關之首長及各級業務主管人員，應負責督導所屬人員之資通安全作業，防範不法及不當行為。
 5. 專業人力資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

(二) 經費配置

1. 資通安全推動小組於規劃配置相關經費及資源時，應考量本機關之資通安全政策及目標，並提供建立、實行、維持及持續改善資通安全維護計

畫所需之資源。

1. 各單位於規劃建置資通系統建置時，應一併規劃資通系統之資安防護需求，並於整體預算中合理分配資通安全預算所佔之比例。
2. 各單位如有資通安全資源之需求，應配合機關預算規劃期程向資通安全推動小組提出，由資通安全推動小組視整體資通安全資源進行分配，並經資通安全長（資通安全管理代表）核定後，進行相關之建置。
3. 資通安全經費、資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

七、 資訊及資通系統之盤點

(一) 資訊及資通系統盤點

1. 本機關每年辦理資訊及資通系統資產盤點，依管理責任指定對應之資產管理人，並依資產屬性進行分類，分別為資訊資產、軟體資產、實體資產、支援服務資產等。

資訊及資通系統資產項目如下

資產類別	資產項目
------	------

<p>資訊資產 (無個 資)</p>	<p>(1) 業務資料檔案，例如：各組業務檔案。</p> <p>(2) 系統資料檔案，例如：資料庫檔案、應用程式檔案及備份檔案等。</p> <p>(3) 電子化儲存之文件檔案，例如：系統或軟體使用手冊及教育訓練教材等。</p> <p>(4) 書面管理文件，例如：系統文件、使用手冊、各種程序辦法等。</p> <p>(5) 書面紀錄，例如：申請表單等。</p>
<p>軟體資產</p>	<p>(1) 系統軟體，例如：業務資訊系統、公文系統等。</p> <p>(2) 資料庫軟體，例如：ORACLE、SQL Server 等。</p> <p>(3) 套裝軟體，例如：Windows 11、Office 2021 等。</p>
<p>硬體資產</p>	<p>(1) 電腦設備，例如：伺服器、工作站、個人主機、筆記型電腦及平板電腦等。</p> <p>(2) 通訊設備，例如：路由器、網路交換器、數據機、傳真機、印表機及影印機等。</p> <p>(3) 儲存媒體，例如：隨身碟、磁帶、光碟及光碟機等。</p> <p>(4) 其他支援設備，例如：監視器、不斷電系統、空調系統、消防系統、環控系統及機房用發電機等。</p>
<p>服務資產</p>	<p>(1) 一般維運支援性服務，例如：網路專線、光纖專線、市內電話系統、供水服務等。</p> <p>(2) 委外服務，例如：網路安全服務、設備主機維護服務等、校務行政系統等。</p>

人員資產	<ul style="list-style-type: none">(1) 內部同仁，例如：學校同仁、約聘人員及替代役人員等。(2) 外部（常駐型）人員，例如：廠商駐點人員等。
個資資產	<ul style="list-style-type: none">(1) 紙本個資，例如：通訊錄、報名表、履歷表等。(2) 檔案形式個資，例如：個人電腦中或主機內個人資料檔案等。(3) 資料庫個資，例如：資訊系統含有個人資料資料庫等。

1. 本機關每年度應依資訊及資通系統盤點結果，製作「資訊及資通系統資產清冊」，欄位應包含：資訊及資通系統名稱、資產名稱、資產類別、擁有者、管理者、使用者、存放位置、防護需求等級。
2. 資訊及資通系統資產應以標籤標示於設備明顯處，並載明財產編號、保管人、廠牌、型號等資訊。
3. 各單位管理之資訊或資通系統如有異動，應即時通知資通安全推動小組更新資產清冊。

(二) 機關資通安全責任等級分級

本機關自行辦理資通業務，未維運自行或委外開發之資通系統者，其資通安全責任等級為 D 級。

八、資通安全風險評估

- (一) 本機關應每年針對資訊及資通設備資產進行風險評估。
- (二) 執行風險評估時應參考臺北市政府教育局「資訊資產風險評鑑管理辦法」執行相關作業。
- (三) 本機關應每年依據資通安全責任等級分級辦法之規定，分別就機密性、完整性、可用性、法律遵循性等構面評估。

九、資通安全防護及控制措施

本機關依據前章資通安全風險評估結果、自身資通安全責任等級之應辦事項，全機關之防護及控制措施詳如本機關資通安全維護計畫，採行相關之防護及控制措施如下：

1. 資訊及資通設備之使用

- (1) 本機關同仁使用資訊及資通設備須遵守設備管理機關相關規範。
- (2) 本機關同仁使用資訊及資通設備時，應留意其資通安全要求事項，並負對應之責任。
- (3) 本機關同仁使用資訊及資通設備後，應依規定之程序歸還。資訊類資訊之歸還應確保相關資訊已正確移轉，並安全地自原設備上抹除。
- (4) 非本機關同仁使用本機關之資訊及資通設備，應確實遵守本機關之相關資通安全要求，且未經授權不得任意複製資訊。
- (5) 對於資訊及資通設備，宜識別並以文件記錄及實作可被接受使用之規則。

(二) 存取控制與加密機制管理

1. 網路安全控管

- (1) 本機關之防火牆由本機關自行管理，區域劃分如下：
 - I 外部網路：對外網路區域，連接外部廣網路(Wide Area Network, WAN)。
 - II 內部區域網路(Local Area Network, LAN)：機關內部單位人員及內部伺服器使用之網路區段。
- (2) 外部網路及內部區域網路間連線需經防火牆進行存取控制，非允許

的服務與來源不能進入其他區域。

(1) 本機關應定期檢視防火牆政策是否適當。

(2) 本機關內部網路之區域應做合理之區隔，使用者應經授權後在授權之範圍內存取網路資源。

(3) 對網路系統管理人員或資通安全主管人員的操作，均應建立詳細的紀錄。並應定期檢視網路安全相關設備設定規則與其日誌紀錄，並檢討執行情形。

(4) 使用者應依機關規定之方式存取網路服務。

(5) 網域名稱系統（DNS）防護

I 一般伺服器應關閉 DNS 服務，防火牆政策亦應針對 DNS 進行控管，關閉不需要的 DNS 服務存取。

II DNS 伺服器應經常性進行弱點漏洞管理與修補、落實存取管控機制。

III 內部主機位置查詢應指向機關內部 DNS 伺服器。

(6) 無線網路防護

I 機密資料原則不得透過無線網路及設備存取、處理或傳送。

II 無線設備應具備安全防護機制以降低阻斷式攻擊風險，且無線網路之安全防護機制應包含外來威脅及預防內部潛在干擾。

III 行動通訊或紅外線傳輸等無線設備原則不得攜入涉及或處理機密資料之區域。

IV. 用以儲存或傳輸資料且具無線傳輸功能之個人電子設備與工作站，應安裝防毒軟體，並定期更新病毒碼。

2. 資通業務權限管理

(1) 本機關之資通業務應設置通行碼管理，通行碼之要求需滿足：

I 通行碼長度 8 碼以上。

II 通行碼複雜度應包含英文大寫小寫、特殊符號或數字三種以上。

III 使用者每 90 天應更換一次通行碼。

(2) 使用者辦理資通業務前應經授權，並使用唯一之使用者 ID，除有特殊營運或作業必要經核准並紀錄外，不得共用 ID。

(3) 使用者無繼續辦理資通業務時，應立即停用或移除使用者 ID，資通業務管理者應定期清查使用者之權限。

3. 特權帳號之存取管理

(1) 資通設備之特權帳號請應經正式申請授權方能使用，特權帳號授權前應妥善審查其必要性，其授權及審查記錄應留存。

(2) 資通設備之特權帳號不得共用。

(3) 對於特權帳號，宜指派與該使用者日常公務使用之不同使用者 ID。

(4) 特權帳號應妥善管理，並應留存特殊權限帳號之使用軌跡。

(5) 資通設備之管理者每季應清查系統特權帳號並劃定特權帳號逾期之處理方式。

4. 加密管理

(1) 本機關之機密資訊於儲存或傳輸時應進行加密。

(2) 本機關之加密保護措施應遵守下列規定：

I 應落實使用者更新加密裝置並備份金鑰。

II 應避免留存解密資訊。

III 一旦加密資訊具遭破解跡象，應立即更改之。

(三) 作業與通訊安全管理

1. 防範惡意軟體之控制措施

(1) 本機關之主機及個人電腦應安裝防毒軟體，並時進行軟、硬體之必要更新或升級。

I. 經任何形式之儲存媒體所取得之檔案，於使用前應先掃描有無惡意軟體。

II. 電子郵件附件及下載檔案於使用前，宜於他處先掃描有無惡意軟體。

III. 確實執行網頁惡意軟體掃描。

(2) 管理者應每年定期針對管理之設備進行軟體清查。

(3) 使用者不得私自使用已知或有嫌疑惡意之網站。

(4) 使用者應定期進行作業系統及軟體更新，以避免惡意軟體利用系統或軟體漏洞進行攻擊。

2. 遠距工作之安全措施

(1) 本機關資通業務之操作及維護以現場操作為原則，避免使用遠距工作，如有緊急需求時，應申請並經資通安全推動小組同意後始可開通。

(2) 資通安全推動小組應定期審查已授權之遠距工作需求是否適當。

(3) 針對遠距工作之連線應採適當之防護措施（並包含伺服器端之集中過濾機制檢查使用者之授權），並且記錄其登入情形。

I. 提供適當通訊設備，並指定遠端存取之方式。

II. 提供虛擬桌面存取，以防止於私有設備上處理及儲存資訊。

III. 遠距工作終止時之存取權限撤銷，並應返還相關設備。

3. 電子郵件安全管理

(1) 使用者使用電子郵件時應提高警覺，並使用純文字模式瀏覽，避免讀取來歷不明之郵件或含有巨集檔案之郵件。

(2) 原則不得電子郵件傳送機密性或敏感性之資料，如有業務需求者應依相關規定進行加密或其他之防護措施。

(3) 使用者不得利用機關所提供電子郵件服務從事侵害他人權益或違法之行為。

(4) 使用者應確保電子郵件傳送時之傳遞正確性。

(5) 本機關應配合上級機關辦理電子郵件社交工程演練，並檢討執行情形。

4. 確保實體與環境安全措施

(1) 通訊機房（機櫃）之管理

I. 通訊機房（機櫃）應進行實體隔離。

II. 機關人員或來訪人員應申請及授權後方可進入通訊機房（機櫃），通訊機房（機櫃）管理者並應定期檢視授權人員之名單。

III. 人員進入管制區應配戴身分識別之標示，並隨時注意身分不明或可疑人員。

IV. 僅於必要時，得准許外部支援人員進入通訊機房（機櫃）。

V. 人員及設備進出通訊機房（機櫃）應留存記錄。

(2) 通訊機房（機櫃）之環境控制

- I. 通訊機房（機櫃）之空調、電力得建立備援措施。
- II. 通訊機房（機櫃）得安裝之安全偵測及防護措施，包括熱度及煙霧偵測設備、火災警報設備、溫濕度監控設備、漏水偵測設備、入侵者偵測系統，以減少環境不安全引發之危險。
- III. 各項安全設備應定期執行檢查、維修，並應定時針對設備之管理者進行適當之安全設備使用訓練。

(3) 辦公室區域之實體與環境安全措施

- I. 應考量採用辦公桌面的淨空政策，以減少文件及可移除式媒體等在辦公時間之外遭未被授權的人員取用、遺失或是被破壞的機會。
- II. 文件及可移除式媒體在不使用或不上班時，應存放在櫃子內。
- III. 機密性及敏感性資訊，不使用或下班時應該上鎖。
- IV. 機密資訊或處理機密資訊之資通業務應避免存放或設置於公眾可接觸之場域。
- V. 顯示存放機密資訊或具處理機密資訊之資通業務地點之通訊錄及內部人員電話簿，不宜讓未經授權者輕易取得。
- VI. 資訊或資通業務相關設備，未經管理人授權，不得被帶離辦公室。

5. 資料備份

- (1) 重要資料應進行資料備份，其備份之頻率應滿足復原時間點目標之要求，並執行異地存放。
- (2) 本機關應每季確認重要資料備份之有效性。且測試該等資料備份時，宜於專屬之測試系統上執行，而非直接於覆寫回原資通設備。
- (3) 敏感或機密性資訊之備份應加密保護。

6. 媒體防護措施

- (1) 使用隨身碟或磁片等存放資料時，具機密性、敏感性之資料應與一般資料分開儲存，不得混用並妥善保管。
- (2) 資訊如以實體儲存媒體方式傳送，應留意實體儲存媒體之包裝，選擇適當人員進行傳送，並應保留傳送及簽收之記錄。
- (3) 為降低媒體材質劣化之風險，宜於所儲存資訊因相關原因而無法讀取前，將其傳送至其他媒體。
- (4) 對機密與敏感性資料之儲存媒體實施防護措施，包含機密與敏感之紙本或備份磁帶，應保存於上鎖之櫃子，且需由專人管理鑰匙。

7. 電腦使用之安全管理

- (1) 電腦、業務系統或自然人憑證，若超過十五分鐘不使用時，應立即登出或啟動螢幕保護功能並取出自然人憑證。
- (2) 禁止私自安裝點對點檔案分享軟體及未經合法授權軟體。
- (3) 連網電腦應隨時配合更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。
- (4) 筆記型電腦及實體隔離電腦應定期以人工方式更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。
- (5) 下班時應關閉電腦及螢幕電源。
- (6) 如發現資安問題，應主動循機關之通報程序通報。
- (7) 支援資訊作業的相關設施如影印機、傳真機等，應安置在適當地點，以降低未經授權之人員進入管制區的風險，及減少敏感性資訊遭破解或洩漏之機會。

8. 行動設備之安全管理

- (1) 機密資料不得由未經許可之行動設備存取、處理或傳送。
- (2) 機敏會議或場所不得攜帶未經許可之行動設備進入

(四) 資通安全防護設備

1. 本機關應建置防毒軟體、網路防火牆、電子郵件過濾裝置，持續使用並

適時進行軟、硬體之必要更新或升級。

2. 資安設備應定期備份日誌紀錄，定期檢視並由主管複核執行成果，並檢討執行情形。

十、資通安全事件通報、應變及演練相關機制

為即時掌控資通安全事件，並有效降低其所造成之損害，本機關應訂定資通安全事件通報、應變及演練相關機制，詳資通安全事件通報應變程序。

十一、資通安全情資之評估及因應

本機關接獲資通安全情資，應評估該情資之內容，並視其對本機關之影響、本機關可接受之風險及本機關之資源，決定最適當之因應方式，必要時得調整資通安全維護計畫之控制措施，並做成紀錄。

1. 資通安全情資之分類評估

本機關接受資通安全情資後，應指定資通安全專責(兼職)人員進行情資分析，並依據情資之性質進行分類及評估，情資分類評估如下：

(1) 資通安全相關之訊息情資

資通安全情資之內容如包括重大威脅指標情資、資安威脅漏洞與攻擊手法情資、重大資安事件分析報告、資安相關技術或議題之經驗分享、疑似存在系統弱點或可疑程式等內容，屬資通安全相關之訊息情資。

(2) 入侵攻擊情資

資通安全情資之內容如包含特定網頁遭受攻擊且證據明確、特定網頁內容不當且證據明確、特定網頁發生個資外洩且證據明確、特定系統遭受入侵且證據明確、特定系統進行網路攻擊活動且證據明確等內容，屬入侵攻擊情資。

(3) 機敏性之情資

資通安全情資之內容如包含姓名、出生年月日、國民身份證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病例、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接識別之個人資料，或涉及個人、法人或團體營業上秘密或經營事業有關之資訊，或情資之公開或提供有侵害公務機關、個人、法人或團體之權利或其他正當利益，或涉及一般公務機密、敏感資訊或國家機密等內容，屬機敏性之情資。

(4) 涉及核心業務、核心資通系統之情資

資通安全情資之內容如包含機關內部之核心業務資訊、核心資通系統、涉及關鍵基礎設施維運之核心業務或核心資通系統之運作等內容，屬涉及核心業務、核心資通系統之情資。

2. 資通安全情資之因應措施

本機關於進行資通安全情資分類評估後，應針對情資之性質進行相應之措施，必要時得調整資通安全維護計畫之控制措施。

(1) 資通安全相關之訊息情資

由資通安全推動小組（資訊小組）彙整情資後進行風險評估，並依據資通安全維護計畫之控制措施採行相應之風險預防機制。

(2) 入侵攻擊情資

由資通安全專責人員判斷有無立即之危險，必要時採取立即之通報應變措施，並依據資通安全維護計畫採行相應之風險防護措施，另通知各單位進行相關之預防。

3. 機敏性之情資

就涉及個人資料、營業秘密、一般公務機密、敏感資訊或國家機密之內容，應採取遮蔽或刪除之方式排除，例如個人資料及營業秘密，應以遮蔽或刪除該特定區段或文字，或採取去識別化之方式排除之。

4. 涉及核心業務、核心資通系統之情資

資通安全推動小組應就涉及核心業務、核心資通系統之情資評估其是否對於機關之運作產生影響，並依據資通安全維護計畫採行相應之風險管理機制。

十二、 資通系統或服務委外辦理之管理

本校目前無委外辦理資通系統之建置、維運或資通服務之提供，若另有需求時得應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。

十三、 資通安全教育訓練

1. 資通安全教育訓練要求

(1) 資安兼任或資訊人員每人每年至少接受 6 小時以上之資安專業課程訓練。

(2) 本機關之一般使用者與主管，每人每年接受 3 小時以上之一般資通安全教育訓練。

2. 資通安全教育訓練辦理方式

(1) 承辦單位應於每學年年初，考量管理、業務及資訊等不同工作類別之需求，擬定資通安全認知宣導及教育訓練計畫，以建立員工資通安全認知，提升機關資通安全

水準，並應保存相關之資通安全認知宣導及教育訓練紀錄 7。

(2) 本機關資通安全認知宣導及教育訓練之內容得包含：

I. 資通安全政策（含資通安全維護計畫之內容、管理程序、流程、要求事項及人員責任、資通安全事件通報程序等）。

II. 資通安全法令規定。

III. 資通安全作業內容。

IV. 資通安全技術訓練。

(3) 員工報到時，應使其充分瞭解本機關資通安全相關作業規範及其重要性。

(4) 資通安全教育及訓練之政策，除適用所屬員工外，對機關外部的使用者，亦應一體適用。

十四、 公務機關所屬人員辦理業務涉及資通安全事項之考核機制

本機關所屬人員之平時考核或聘用，依據公務機關所屬人員資通安全事項獎懲辦法、臺北市政府及所屬各機關學校公務人員平時獎懲標準表、臺北市國民小學組織規程規定辦理之。

十五、 資通安全維護計畫及實施情形之持續精進及績效管理機制

1. 資通安全維護計畫之實施

為落實本安全維護計畫，使本機關之資通安全管理有效運作，相關單位於訂定各階文件、流程、程序或控制措施時，應與本機關之資通安全政策、目標及本安全維護計畫之內容相符，並應保存相關之執行成果記錄。

2. 資通安全維護計畫實施情形之稽核機制

(1) 稽核機制之實施

I. 資通安全推動小組應定期（至少每年一次）或於系統重大變更或組織改造後執行一次內部稽核作業，以確認人員是否遵循本規範與機關之管理程序要求，並有效實作及維持管理制度。

II. 辦理稽核前資通安全推動小組應擬定資通安全稽核計畫並安排稽核成員，稽核計畫應包括稽核之依據與目的、期間、重點領域、稽核小組組成方式、保密義務、稽核方式、基準與項目及受稽單位協助事項，並應將前次稽核之結果納入稽核範圍。

III. 辦理稽核時，資通安全推動小組應於執行稽核前 14 日，通知受

稽核單位，並將稽核期程、稽核項目紀錄表及稽核流程等相關資訊提供受稽單位。

IV. 本機關之稽核人員應受適當培訓並具備稽核能力，且不得稽核自身經辦業務，以

確保稽核過程之客觀性及公平性；另於執行稽核時，應填具稽核項目紀錄表，待稽核結束後，應將稽核項目紀錄表內容彙整至稽核結果及改善報告中，並提供給受稽單位填寫辦理情形。

V. 稽核結果應對相關管理階層（含資安長）報告，並留存稽核過程之相關紀錄以作為資通安全稽核計畫及稽核事件之證據。

VI. 稽核人員於執行稽核時，應至少執行一項特定之稽核項目（如是否瞭解資通安全政策及應負之資安責任、是否訂定人員之資通安全作業程序與權責、是否定期更改密碼）。

(2) 稽核改善報告

I. 受稽單位於稽核實施後發現有缺失或待改善項目者，應對缺失或待改善之項目研議改善措施、改善進度規劃，並落實執行。

II. 受稽單位於稽核實施後發現有缺失或待改善者，應判定其發生之原因，並評估是否有其類似之缺失或待改善之項目存在。

III. 受稽單位於判定缺失或待改善之原因後，應據此提出並執行相關之改善措施及改善進度規劃，必要時得考量對現行資通安全管理制度或相關文件進行變更。

IV. 機關應定期審查受稽單位缺失或待改善項目所採取之改善措施、改善進度規劃及佐證資料之有效性。

V. 受稽單位於執行改善措施時，應留存相關之執行紀錄，並填寫稽核結果及改善報

告。

3. 資通安全維護計畫之持續精進及績效管理

(1) 本機關之資通安全推動小組應於每年 10 月底前召開資通安全管理審查會議，確認資通安全維護計畫之實施情形，確保其持續適切性、合宜性及有效性。

(2) 管理審查議題應包含下列討論事項：

I. 過往管理審查議案之處理狀態。

II. 與資通安全管理業務有關之內部及外部議題的變更，如法令變更、上級機關要求、資通安全推動小組決議事項等。

III. 資通安全維護計畫內容之適切性。

IV. 資通安全績效之回饋，包括：

i. 資通安全政策及目標之實施情形。

ii. 資通安全人力及資源之配置之實施情形。

iii. 資通安全防護及控制措施之實施情形。

iv. 內外部稽核結果。

v. 不符合項目及矯正措施。

V. 風險評鑑結果及風險處理計畫執行進度。

VI. 重大資通安全事件之處理及改善情形。

VII. 利害關係人之回饋。

VIII. 持續改善之機會。

(3) 持續改善機制之管理審查應做成改善績效追蹤報告，相關紀錄並應予保存，以作為管理審查執行之證據。

十六、資通安全維護計畫實施情形之提出

本機關依據資通安全管理法第 12 條之規定，應於每年 11 月中向臺北市政府教育局資訊教育科，提出資通安全維護計畫實施情形，使其得瞭解本機關之年度資通安全計畫實施情形。

十七、 相關法規、程序及表單

1. 相關法規及參考文件

(1) 資通安全管理法

(2) 資通安全管理法施行細則

(3) 資通安全責任等級分級辦法

(4) 資通安全事件通報及應變辦法

(5) 資通安全情資分享辦法

(6) 公務機關所屬人員資通安全事項獎懲辦法

(7) 資訊系統風險評鑑參考指引

(8) 政府資訊作業委外安全參考指引

(9) 無線網路安全參考指引

(10) 網路架構規劃參考指引 (11)行政裝置資安防護參考指引

(12)政府行動化安全防護規劃報告(13)安全軟體發展流程指引

(14)安全軟體設計指引(15)安全軟體測試指引

(16) 資訊作業委外安全參考指引

(17) 本機關資通安全事件通報及應變程序

2. 附件表單

(1) 資通安全推動小組成員及分工表

(2) 資通安全保密同意書

(3) 資通安全需求申請單

(4) 資訊及資通資產清冊

(5) 風險評估表

- (6) 風險類型暨風險對策參考表
- (7) 管制區域人員進出登記表
- (8) 委外廠商執行人員保密切結書、保密同意書
- (9) 委外廠商查核項目表
- (10) 年度資通安全教育訓練計畫
- (11) 資通安全認知宣導及教育訓練簽到表
- (12) 資通安全維護計畫實施情形(13)資通安全稽核計畫
- (14)稽核項目紀錄表(15)稽核結果紀錄表
- (16)稽核委員聘任同意保密切結書(17)稽核結果及改善報告
- (18)改善績效追蹤報告

臺北北投區石牌國民小學資通安全維護計畫附件

目次

臺北市北投區石牌國民小學資通安全推動小組成員及分工表.....	2
臺北市北投區石牌國民小學資通安全保密同意書.....	4
臺北市北投區石牌國民小學資通安全需求申請單.....	5
臺北市北投區石牌國民小學資訊及資通資產清冊.....	6
臺北市北投區石牌國民小學資訊安全風險評估表.....	9
臺北市北投區石牌國民小學資安風險類型暨對策參考表.....	10
臺北市北投區石牌國民小學管制區域人員進出登記表.....	12
臺北市北投區石牌國民小學委外廠商執行人員保密切結書.....	13
臺北市北投區石牌國民小學委外廠商執行人員保密同意書.....	15
臺北市北投區石牌國民小學委外廠商保密切結書.....	17
臺北市北投區石牌國民小學委外廠商查核項目表.....	18
臺北市北投區石牌國民小學人員申請遠距工作保密切結書.....	23
臺北市北投區石牌國民小學資通安全教育訓練計畫.....	24
臺北市北投區石牌國民小學資通安全認知宣導教育訓練簽到表.....	26
臺北市北投區石牌國民小學資通安全維護計畫實施情形.....	27
臺北市北投區石牌國民小學稽核項目紀錄表.....	32
臺北市北投區石牌國民小學稽核委員聘任同意暨保密切結書.....	33
臺北市北投區石牌國民小學稽核結果及改善報告.....	35
臺北市北投區石牌國民小學改善績效追蹤報告.....	36

1. 資通安全推動小組成員及分工表

臺北市北投區石牌國民小學資通安全推動小組成員及分工表

編號：

製表日期： 年 月 日

單位職級	組別	職掌事項	分機	代理人
校長	策略規劃組	1. 學校資訊安全推動小組召集人 2. 統籌及督導資訊安全業務 3. 學校資訊安全推動小組資安長	188	教務主任
教務主任	績效管理組	1. 推動全校資訊安全工作相關業務 2. 資訊安全第一聯絡人	111	教學組長
學務主任		督導學生事務相關資訊安全工作	221	生教組長
總務主任		1. 支援校園資訊安全相關庶務工作 2. 經費請購與設備採買事宜	331	事務組長
輔導主任		督導學生輔導相關資訊安全工作	551	輔導組長
幼兒園主任		督導幼兒園相關資訊安全工作	170	幼兒園 教學組長
人事主任		辦理資通安全內部稽核工作	661	人事書記
會計主任		資訊安全工作相關經費核銷事宜	663	會計佐理 員
資訊小組學年 代表		1. 協助溝通傳達校園資訊安全工作事宜	無	各學年教 師

資訊 組長	資安 管理組	<ol style="list-style-type: none"> 1. 資訊安全第二聯絡人 2. 資安事件通報與處理 3. 校園網路安全工作 4. 防火牆管理及網路流量監控 5. 行政及教學電腦防毒防駭 6. 校內電腦作業系統及病毒碼定期更新 7. 辦理教師及學生資訊安全、相關法令之研習宣導 8. 其他相關資訊安全業務 	1 15	系統 管理師
系統管理師		<ol style="list-style-type: none"> 1. 資通安全事件通報 2. 資訊設備維作運護 	115	資訊組長

承辦人：

單位業務主管：

資通安全長：

2.資通安全保密同意書

臺北市北投區石牌國民小學資通安全保密同意書

編號：

立同意書人_____於民國____年____月____日起於

__任職，因業務涉及單位重要之資訊及資通系統，故同意下列保密事項：

一、於業務上所知悉之機敏資料及運用之資通系統等，應善盡保管及保密之責。二、相關業務之資訊、文件，不得私自洩漏與業務無關之人員。

三、遵守其他本單位資通安全相關之法令及規定。

四、如有危害本單位資通安全之行為，願負相關之責任。

立同意書人：_____ (簽章) 身

份證字號：_____ 服務機

關：_____

機關首長：_____

中華民國 年 月 日

3. 資通安全需求申請單

臺北市北投區石牌國民小學資通安全需求申請單

編號：

申請單位		申請日期	年 月 日		
申請項目	<input type="checkbox"/> 軟體 <input type="checkbox"/> 硬體 <input type="checkbox"/> 其他	項目名稱			
申請數量		需用日期	年 月 日		
申請類別	<input type="checkbox"/> 新購 <input type="checkbox"/> 升級	使用設備	<input type="checkbox"/> 主機 <input type="checkbox"/> 使用者電腦 <input type="checkbox"/> 其他		
安裝單位		安裝位置			
用途說明					
申請人		申請單位主管			
資通安全推動小組	<input type="checkbox"/> 可採購 <input type="checkbox"/> 不可採購	說明：			
資通安全推動小組承辦人員		單位業務主管		資通安全長	

5.風險評估表

臺北市北投區石牌國民小學資訊安全風險評估表

編號：

製表日期： 年 月 日

風險列表	風險評估				發生可能性	影響後果	風險等級	管理機制
	機密性	完整性	可用性	法律遵循性				
(略)								

承辦人員：

單位主管：

6.風險類型暨風險對策參考表

臺北市北投區石牌國民小學資安風險類型暨對策參考表

作業內容	具體風險類型	風險處理對策
網際網路探尋	網頁搜尋	強化網頁伺服器，避免存放 index.html、default.asp 的檔案資料夾，並禁用相關的目錄索引。使用 robots.txt 指示搜尋引擎不要為其內容編制索引。
	WHOIS 查詢	在 WHOIS 資料庫及 TLS 憑證中，使用平常、單一的網路管理人聯絡資訊，以降低社交工程與撥號攻擊的成功率。
	DNS 查詢	設定 DNS 伺服器，禁止其對不可信任的主機執行區域轉送，並主動從網際網路掃描 TCP 和 UDP 的端口 53，以便發現是否有偽冒的名稱伺服器。刪減 DNS 區域檔案內容，以防洩漏不必要的訊息，例如非公開的 IP 位址和主機名稱，並且於必要時才使用 PTR 紀錄。
	SMTP 探尋	設定 SMTP 伺服器在遇到問題時，例如寄件人不存在時，不要發送 NDN，以防攻擊者藉機列舉內部郵件系統及組態內容。
區域網路攻擊	MITM 和偽冒伺服器攻擊	強制採用傳輸層安全加密與透過具有憑證檢驗功能的身份驗證機制
	802.1X 攻擊	<ul style="list-style-type: none"> ● 檢測 X.509 憑證是否有效。 ● 指定合法驗證者 (RADIUS 伺服器) 之一般名稱值。 ● 在安全功能發生問題時，禁止提供詳細資訊給終端使用者，以提高故障安全性。
	資料連結層攻擊	<ul style="list-style-type: none"> ● 將交換連接埠設為 access 模式，並關閉動態建立主幹網路的功能。 ● 關閉未用到的乙太網路連接埠，並歸類在隔離的 VLAN 外。
	網路層與應用層的攻擊	<ul style="list-style-type: none"> ● 如果沒有明確要求，應關閉 IPv6。 ● 取消對 ICMP 重導向的支援。 ● 停用群播名稱解析及 Windows 的 NetBIOS over TCP/IP 通訊。
網路服務漏洞	網路攻擊表面	將不必要的功能關閉。
	伺服器套件包與程式庫攻擊	隨時修補存在攻擊表面的已知攻擊。
	透過傳輸與遠端維護操作之服務進行攻擊	<ul style="list-style-type: none"> ● 停用無加密傳輸安全性的 Telnet、FTP、SNMP、VNC 等。 ● 遠端操作維護須透過安全的身份驗證連接。 ● 建構封閉的管理網路。

	SSH 伺服器攻擊	<ul style="list-style-type: none"> ● 強制使用 2.0 版本的協定，禁止向下相容特性。 ● 停用使用者的密碼驗證機制，強制使用者採取一次性密碼（OTP）、公鑰或多因子驗證，例如可透過 Google Authenticator、Duo Security 或其他平台取得。
	DNS 伺服器攻擊	<ul style="list-style-type: none"> ● 停止支援來自不受信任來源的遞回查詢。 ● 確保區域檔案不含多餘或敏感資訊。
	Kerberos 伺服器攻擊	<p>停止支援較弱的 HMAC 演算法。</p> <ul style="list-style-type: none"> ● 在微軟環境中，可考慮強制使用最高的網域功能等級。
VPN 服務 (暫無)	VPN 攻擊	<ul style="list-style-type: none"> ● 確認 VPN 伺服器的維護作業，並修補到最新版本。 ● 強制使用 AH 和 ESP 功能身份驗證及機密性服務。 ● 使用數位憑證取代預置共享金鑰，並要求對設備進行身份驗證。 ● 過濾內連的 VPN 流量，以便在發生入侵事件時限制網路存取。 ● 定期稽核已授權的 VPN 使用者，以防有偽冒的帳號。
網頁應用程式框架	Web 應用伺服器攻擊	<ul style="list-style-type: none"> ● 確保應用程式框架組件都已修補至最新版本，包括相依與間接使用的組件。 ● 禁止將管理介面或特權功能公開在不受信任的網路上。 ● 在可行的情況下，將開放網頁應用程式和管理功能隔離。
資料儲存機制	資料庫攻擊	<ul style="list-style-type: none"> ● 限制資料服務只與經授權的對象往來，特別是雲端環境中。 ● 避免使用不支援身份驗證的儲存系統和協定。 ● 禁止在可公開讀取的儲存裝置，例如 NFS、iSCSI、SMB 和 AFP 等，以未加密狀態儲存機敏資料，包括系統和資料庫的備份檔案通常存有機敏資料，例如密碼、身份憑證。 ● 確保密碼強度。 ● 限制只有受信任的網路才能存取管理服務。 ● 稽查和監控身份驗證事件，識別濫用身份憑據和暴力拆解密碼的情形。
參考來源：資安風險評估指南，第三版，Chris McNab，江湖海譯。		

7.管制區域人員進出登記表

臺北市北投區石牌國民小學管制區域人員進出登記表

編號：

製表日期： 年 月 日

編號	單位姓名	配同人員	日期	進出時間	事由	進出設備(物品)
1	單位：姓名：			進去：離 去：		
2	單位：姓名：			進去：離 去：		
3	單位：姓名：			進去：離 去：		
4	單位：姓名：			進去：離 去：		
5	單位：姓名：			進去：離 去：		
6	單位：姓名：			進去：離 去：		
7	單位：姓名：			進去：離 去：		
8	單位：姓名：			進去：離 去：		
9	單位：姓名：			進去：離 去：		
10	單位：姓名：			進去：離 去：		

承辦人員： 單位主管：

8. 委外廠商執行人員保密切結書、保密同意書

臺北市北投區石牌國民小學委外廠商執行人員保密切結書

立切結書人_____（簽署人姓名）等，受_____（廠商名稱）委派至_____（機關名稱，以下稱機關）處理業務，謹聲明恪遵機關下列工作規定，對工作中所持有、知悉之資訊系統作業機密或敏感性業務檔案資料，均保證善盡保密義務與責任，非經機關權責人員之書面核准，不得擷取、持有、傳遞或以任何方式提供給無業務關係之第三人，如有違反願賠償一切因此所生之損害，並擔負相關民、刑事責任，絕無異議。

一、未經申請核准，不得私自將機關之資訊設備、媒體檔案及公務文書攜出。

二、未經機關業務相關人員之確認並代為申請核准，不得任意將攜入之資訊設備連接機關網路。若經申請獲准連接機關網路，嚴禁使用數據機或無線傳輸等網路設備連接外部網路。

三、經核准攜入之資訊設備欲連接機關網路或其他資訊設備時，須經電腦主機房掃毒專責人員進行病毒、漏洞或後門程式檢測，通過後發給合格標籤，並將其粘貼在設備外觀醒目處以備稽查。

四、廠商駐點服務及專責維護人員原則應使用機關配發之個人電腦與週邊設備，並僅開放使用機關內部網路。若因業務需要使用機關電子郵件、目錄服務，應經機關業務相關人員之確認並代為申請核准，另欲連接網際網路亦應經機關業務相關人員之確認並代為申請核准。

五、機關得定期或不定期派員檢查或稽核立切結書人是否符合上列工作規定。

六、本保密切結書不因立切結書人離職而失效。

七、立切結書人因違反本保密切結書應盡之保密義務與責任致生之一切損害，立切結書人所屬公司或廠商應負連帶賠償責任。

立切結書人：

姓名及簽章

身分證字號

聯絡電話及戶籍地址

_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

立切結書人所屬廠商：

廠商名稱及蓋章

廠商負責人姓名及簽章

廠商聯絡電話及地址

_____	_____	_____
-------	-------	-------

填表說明：

- 一、廠商駐點服務人員、專責維護人員，或逗留時間超過三天以上之突發性維護增援、臨時性系統測試或教育訓練人員（以授課時需連結機關網路者為限）及經常到機關洽公之業務人員皆須簽署本切結書。
- 二、廠商駐點服務人員、專責維護人員及經常到機關洽公之業務人員每年簽署本切結書乙次。

中華民國 年 月 日

臺北市北投區石牌國民小學委外廠商執行人員保密同意書

茲緣於簽署人 (簽署人姓名，以下稱簽署人)參與.....

(廠商名稱，以下稱廠商)得標..... (機關名稱)以下稱機關)資通業務委外案..... (案名)以下稱「本案」)於本案執行期間有知悉或可得知悉或持有政府公務秘密及業務秘密，為保持其秘密性，簽署人同意恪遵本同意書下列各項規定：

第一條 簽署人承諾於本契約有效期間內及本契約期滿或終止後，對於所得知或持有一切機關未標示得對外公開之公務秘密，以及機關依契約或法令對第三人負有保密義務之業務秘密，均應以善良管理人之注意妥為保管及確保其秘密性，並限於本契約目的範圍內，於機關指定之處所內使用之。非經機關事前書面同意，不得為本人或任何第三人之需要而複製、保有、利用該等秘密或將之洩漏、告知、交付第三人或以其他任何方式使第三人知悉或利用該等秘密，或對外發表或出版，亦不得攜至機關或機關所指定處所以外之處所。

第二條 簽署人知悉或取得機關公務秘密與業務秘密應限於其執行本契約所必需且僅限於本契約有效期間內。簽署人同意公務秘密與業務秘密，應僅提供、告知有需要知悉該秘密之履約廠商團隊成員人員。

第三條 簽署人在下述情況下解除其所應負之保密義務：
原負保密義務之資訊，由機關提供以前，已合法持有或已知且無保密必要者。

原負保密義務之資訊，依法令業已解密、依契約機關業已不負保密責任、或已為公眾所知之資訊。

原負保密義務之資訊，係自第三人處得知或取得，該第三人就該等資訊並無保密義務。

而失其效力。

第六條 本同意書一式叁份，機關、簽署人及_____（廠商）各執存一份。

簽署人姓名及簽章：身分證字號：

聯絡電話：戶籍地

址：

所屬廠商名稱及蓋章：所屬廠商負責人姓

名及簽章：所屬廠商地址：

中 華 民 國 年 月 日

9. 委外廠商保密切結書

臺北市北投區石牌國民小學委外廠商保密切結書

編號：

公司(以下簡稱乙方) 承攬臺北市北投區石牌國民小學(以下簡稱甲方) 「 (填寫服務名稱)」(以下簡稱本專案)，於執行過程中，乙方自甲方所取得之公務(機密)資訊，具結依下列規定保密並履行責任：

一、乙方應遵守「電腦處理個人資料保護法」、「刑法」、「行政院及所屬各機關資訊安全管理要點」、「行政院及所屬各機關資訊安全管理規範」等

相關法令，不私自蒐集本專案範圍外任何資訊。

二、乙方於本專案進行期間，依契約所產生或接觸之公務(機密)資料，，非經甲方同意或授權，不得以任何形式洩漏或將上開資料再使用或交付第三人。對所獲得或知悉之上述公務(機密)資料，乙方須負保密責任。其因法令或主管機關規定需向公務機關提供時，應在第一時間通知甲方。

三、公務（機密）資料保密期限，不受本專案工作完成（結案）及乙方不同工作地點及時間之限制。乙方持有或獲知公務（機密）資料，不得洩漏或轉讓於第三人。若因本專案終止，公務（機密）資料無再使用之必要，乙方應進行資料銷毀，不得以任何形式保存。

四、乙方違反本資訊安全保密切結書之規定，致造成甲方或第三人之損害或賠償，乙方同意無條件負擔全部責任，包括因此所致甲方或第三人涉訟，所須支付之一切費用及賠償。於第三人對甲方提出請求、訴訟，經甲方以書面通知乙方提供相關資料，乙方應合作提供，絕無異議。

此致

臺北市北投區石牌國民小學立切結書人

廠商名稱及蓋章：

廠商負責人姓名及簽章： 統一編號：

公司地址：

中 華 民 國 年 月 日

10.委外廠商查核項目表臺北市北投區石牌國民小學委外廠商查核項目表

編號：

填表日期： 年 月 日 查核人員：

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
1. 資通安全政策之推動及目標訂定	1.1 是否定義符合組織需要之資通安全政策及目標？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	已訂定資通安全政策及目標。
	1.2 組織是否訂定資通安全政策及目標？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	政策及目標符合機關之需求。
	1.3 組織之資通安全政策文件是否由管理階層核准並正式發布且轉知所有同仁？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	依規定按時進行教育訓練之宣達。
	1.4 組織是否對資通安全政策、目標之適切性及有效性，定期作必要之審查及調整？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	定期進行政策及目標之檢視、調整。
	1.5 是否隨時公告資通安全相關訊息？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	將資安訊息公告於布告欄。
2. 設置資通安全推動組織	2.1 是否指定適當權責之高階主管負責資通安全管理之協調、推動及督導等事項？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	指派首長擔任資安長。
	2.2 是否指定專人或專責單位，負責辦理資通安全政策、計畫、措施之研議，資料、資通系統之使用管理及保護，資安稽核等資安工作事項？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	有設置內部資通安全推動小組，並制訂相關之權責分工。
	2.3 是否訂定組織之資通安全責任分工？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	機關內部訂有資安責任分工組織。
3. 配置適當之資通安全專業人員及適當之資源	3.1 是否訂定人員之安全評估措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	有訂定人員錄用之安全評估措施
	3.2 是否符合組織之需求配置專業資安人力？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	機關依規定配置資安人員1人。

查核項目	查核內容	查核結果			說明
		合	符	適	
	3.3 是否具備相關專業資安證照或認證？				專業人員具備 ISO27001之證照
	3.4 是否配置適當之資源？				機關並未投入足夠資安資源。
4. 資訊及資通系統之盤點及風險評估	4.1 是否建立資訊及資通系統資產目錄，並隨時維護更新？				依規定建置資產目錄，並定時盤點。
	4.2 各項資產是否有明確之管理者及使用者？				資產依規定指定管理者及使用者。
	4.3 是否定有資訊、資通系統分級與處理之相關規範？				資訊訂有分級處理之作業規範。
	4.4 是否進行資訊、資通系統之風險評估，並採取相應之控制措施？				已進行風險評估及擬定相應之控制措施。
	5.1 人員進入重要實體區域是否訂有安全控制措施？				機房訂有門禁管制措施。
	5.2 重要實體區域的進出權利是否定期審查並更新？				離職人員之權限未刪除。

5. 資通安全管理措施之實施情況	5.3 電腦機房及重要地區，對於進出人員是否作必要之限制及監督其活動？				對於進出人員並未監督其活動。
	5.4 電腦機房操作人員是否隨時注意環境監控系統，掌握機房溫度及溼度狀況？				按時檢測機房物理面之情況。
	5.5 各項安全設備是否定期檢查？同仁有否施予適當的安全設備使用訓練？				依規定定期檢查並按時提供同仁安全設備之使用運練。
	5.6 第三方支援服務人員進入重要實體區域是否經過授權並陪同或監視？				並未陪同或監視第三方支援人員。
	5.7 重要資訊處理設施是否有特別保護機制？				對於核心系統主機並未設置特別保護機制。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
5.8	重要資通設備之設置地點是否檢查及評估火、煙、水、震動、化學效應、電力供應、電磁幅射或民間暴動等可能對設備之危害？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	定期檢查物理面之風險。
5.9	電源之供應及備援電源是否作安全上考量？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	有設置備用電源。
5.10	通訊線路及電纜線是否作安全保護措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	電纜線老舊，並未設有安全保護措施。
5.11	設備是否定期維護，以確保其可用性及完整性？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	設備按期維護。
5.12	設備送場外維修，對於儲存資訊是否訂有安全保護措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	訂有相關之保護措施。
5.13	可攜式的電腦設備是否訂有嚴謹的保護措施(如設通行碼、檔案加密、專人看管)？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	攜帶式設備訂有保護措施。
5.14	設備報廢前是否先將機密性、敏感性資料及版權軟體移除或覆寫？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	設備報廢前均有進行資料清除程序。
5.15	公文及儲存媒體在不使用或不在班時是否妥為存放？機密性、敏感性資訊是否妥為收存？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	人員下班後並未將機敏性公文妥善存放。
5.16	系統開發測試及正式作業是否區隔在不同之作業環境？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	系統開發測試與正式作業區隔。
5.17	是否全面使用防毒軟體並即時更新病毒碼？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	按時更新病毒碼。
5.18	是否定期對電腦系統及資料儲存媒體進行病毒掃描？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	定期進行相關系統之病毒掃描。
5.19	是否定期執行各項系統漏洞修補程式？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	定期進行漏洞修補。
5.20	是否要求電子郵件附件及下載檔案在使用前需檢查有無惡意軟體(含病毒、木馬或後門等程式)？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	系統設有檢查之機制。
5.21	重要的資料及軟體是否定期作備份處理？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	有定期做備份處理。
5.22	備份資料是否定期回復測試，以確保備份資料之有效性？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	備份資料均有測試。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
5.8	重要資通設備之設置地點是否檢查及評估火、煙、水、震動、化學效應、電力供應、電磁幅射或民間暴動等可能對設備之危害？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	定期檢查物理面之風險。
5.9	電源之供應及備援電源是否作安全上考量？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	有設置備用電源。
5.10	通訊線路及電纜線是否作安全保護措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	電纜線老舊，並未設有安全保護措施。
5.11	設備是否定期維護，以確保其可用性及完整性？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	設備按期維護。
5.12	設備送場外維修，對於儲存資訊是否訂有安全保護措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	訂有相關之保護措施。
5.13	可攜式的電腦設備是否訂有嚴謹的保護措施(如設通行碼、檔案加密、專人看管)？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	攜帶式設備訂有保護措施。
5.14	設備報廢前是否先將機密性、敏感性資料及版權軟體移除或覆寫？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	設備報廢前均有進行資料清除程序。
5.15	公文及儲存媒體在不使用或不在班時是否妥為存放？機密性、敏感性資訊是否妥為收存？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	人員下班後並未將機敏性公文妥善存放。
5.16	系統開發測試及正式作業是否區隔在不同之作業環境？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	系統開發測試與正式作業區隔。
5.17	是否全面使用防毒軟體並即時更新病毒碼？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	按時更新病毒碼。
5.18	是否定期對電腦系統及資料儲存媒體進行病毒掃瞄？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	定期進行相關系統之病毒掃瞄。
5.19	是否定期執行各項系統漏洞修補程式？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	定期進行漏洞修補。
5.20	是否要求電子郵件附件及下載檔案在使用前需檢查有無惡意軟體(含病毒、木馬或後門等程式)？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	系統設有檢查之機制。
5.21	重要的資料及軟體是否定期作備份處理？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	有定期做備份處理。
5.22	備份資料是否定期回復測試，以確保備份資料之有效性？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	備份資料均有測試。

查核項目	查核內容	查核結果			說明
		合	符	適	
	5.23 對於敏感性、機密性資訊之傳送是否採取資料加密等保護措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	均有設加密之保護措施。
	5.24 是否訂定可攜式媒體(磁帶、磁片、光碟片、隨身碟及報表等)管理程序？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	訂有可攜式媒體之管理程序。
	5.25 是否訂定使用者存取權限註冊及註銷之作業程序？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	訂有使用者存取權限註冊及註銷之作業程序。
	5.26 使用者存取權限是否定期檢查(建議每六個月一次)或在權限變更後立即複檢？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	未定期檢視使用者存取權限。
	5.27 通行碼長度是否超過 6 個字元(建議以 8 位或以上為宜)？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	通行碼符合規定。
	5.28 通行碼是否規定需有大小寫字母、數字及符號組成？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	通行碼符合規定。
	5.29 是否依網路型態(Internet、Intranet、Extranet)訂定適當的存取權限管理方式？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	依規定訂定適當之存取權限。
	5.30 對於重要特定網路服務，是否作必要之控制措	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	對於特定網路有訂定相關

施，如身份鑑別、資料加密或網路連線控制？				之控制措施。
5.31 是否訂定行動式電腦設備之管理政策(如實體保護、存取控制、使用之密碼技術、備份及病毒防治要求)？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	有針對行動式電腦訂定管理政策。
5.32 重要系統是否使用憑證作為身份認證？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	針對重要系統設有身份認證。
5.33 系統變更後其相關控管措施與程序是否檢查仍然有效？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	系統更新後相關措施仍有 效。
5.34 是否可及時取得系統弱點的資訊並作風險評估及採取必要措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	可即時取得系統弱點並採取應變措施。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
6. 訂定資通安全事件通報及應變之程序及機制	6.1 是否建立資通安全事件發生之通報應變程序？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	有訂定通報應變程序。
	6.2 機關同仁及外部使用者是否知悉資通安全事件通報應變程序並依規定辦理？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	同仁及委外廠商均知悉通報應變程序，並定期宣導。
	6.3 是否留有資通安全事件處理之記錄文件，記錄中並有改善措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	有留存相關紀錄。
7. 定期辦理資通安全認知宣導及教育訓練	7.1 是否定期辦理資通安全認知宣導？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	有定期辦理宣導。
	7.2 是否對同仁進行資安評量？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	按期進行資安評量。
	7.3 同仁是否依層級定期舉辦資通安全教育訓練？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	有定期辦理教育訓練。
	7.4 同仁是否瞭解單位之資通安全政策、目標及應負之責任？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	同仁均瞭解單位之資通安全政策及目標。
8. 資通安全維護計畫實施情形之精進改善機制	8.1 是否設有稽核機制？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	訂有稽核機制。
	8.2 是否定有年度稽核計畫？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	有訂定年度稽核計畫。
	8.3 是否定期執行稽核？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	有按期執行稽核。
	8.4 是否改正稽核之缺失？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	訂有稽核後之缺失改正措施。
9. 資通安全維護計畫及實施情形之績效管考機制	10.1 是否訂定安全維護計畫持續改善機制？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	有訂定持續改善措施。
	10.2 是否追蹤過去缺失之改善情形？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	有追蹤缺失改善之情形。
	10.3 是否定期召開持續改善之管理審查會議？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	定期召開管理審查會議。

單位主管：

資通安全長³：

11 人員申請遠距工作保密切結書

臺北市北投區石牌國民小學人員申請遠距工作保密切結書

編號：_____ - _____

具保密切結（人員）_____（以下簡稱乙方）於民國_____年____月_____

日起於臺北市北投區石牌國小執行因行政業務（或專案）需求，申請使用電

腦遠端桌面連線服務「_____（請填軟體或服務名稱）」（以下簡

稱本服務），使用期間接觸公務(機密)資料，將恪遵以下保密規定：

一、乙方不得將公務(機密)資料以任何形式利用或洩漏、告知、交付、移轉予任何第三人，如有違誤願負法律上之責任。

二、本服務僅限乙方個人使用，乙方應嚴守資安規定，不得將本服務以任何形式轉予第三人使用，如有違誤願負法律上之責任。

此致

臺北市北投區石牌國民小學

具切結書委外（人員）：

（簽章）

12 年度資通安全教育訓練計畫

臺北市北投區石牌國民小學資通安全教育訓練計畫

壹、依據

臺北市北投區石牌國民小學之資通安全維護計畫理。貳、目的

為精進所屬人員之資通安全意識及職能，並敦促該等人員得以瞭解並執行本校之資通安全維護計畫，以強化本校之資通安全管理能量，爰要求該等人員應接受資通安全之教育訓練，爰擬定本教育訓練計畫。

參、實施範圍 本校所屬人員：

人員類別		人數
教師兼資通安全人員		(略)
教師兼資訊人員		
一般主管		
一 般 使 用 者	教師(不含兼任資通人員)	
	職員	
	技工及工友	
	警衛	
共計		

肆、訓練項目

人員類別	訓練課程 4	時數
教師兼資通安全人員 教師兼資訊人員	資通安全管理制度 資訊系統風險管理 資通安全稽核	3
	資安事故處理 業務持續運作管理	
一般主管、使用者	資安基本認知 資通安全管理制度	3

伍、訓練期程

由本校自行排定期程。

陸、訓練方式

由本校自行依課程內容，採取合宜教育訓練方式（實體課程、線上課程.....）。

13. 資通安全認知宣導及教育訓練簽到表

臺北市北投區石牌國民小學

資通安全認知宣導教育訓練簽到表

編號：

課程名稱：_____時間：

地點：_____

單位	職稱	姓名	簽名

14. 資通安全維護計畫實施情形

臺北市北投區石牌國民小學資通安全維護計畫實施情形

編號：

本校之業務因涉及全國性民眾個人資料檔案之持有及處理，經主管機關核定後本單位之資通安全責任等級為 D 級，依資通安全管理法第 12 條之規定，向鈞局提出本年度資通安全維護計畫實施情形、執行成果及說明如下表所示：

實施項目	實施內容	實施情形說明
1. 核心業務及其重要性	1.1 核心業務及重要性盤點	本校核心業務及重要性詳參資通安全維護計畫（詳附件，下同）。
2. 資通安全政策及目標之訂定	2.1 資通安全政策訂定及核定	本校已訂定資通安全政策，詳參資通安全維護計畫，並經資安長核定（詳公文附件）。
	2.2 資通安全目標之訂定	本校已訂定資通安全目標，詳參資通安全維護計畫。
	2.3 資通安全政策及目標宣導	本校為推動資通安全政策，已定期向同仁及利害關係人進行宣達。
	2.4 資通安全政策及目標定期檢視	本校已定期召開資通安全管理審查會議中檢討資通安全政策及目標之適切性（詳會議記錄）。
3. 設置資通安全推動組織	3.1 設定資通安全長	本校已指定校長為資通安全長，其職掌詳參資通安全維護計畫。
	3.2 設置資通安全推動小組	本校已設置資通安全推動小組，其組織、分工及職常詳參資通安全維護計畫。
4. 人力及經費之配置	4.1 專職(責)人員配置	本校依規定配置資通安全兼任人員 1 人。另因其業務內容將涉及機密性資料，故已進行相關安全評估。

	4.2 經費之配置	本校今年視需求已合理分資安經費。
5. 資訊及資通系統之盤點及核心資通系統、相關資產之標示	5.1 資訊及資通系統之盤點 5.2 機關資通安全責任等級分級	本校已於今年 01 月盤點本校之資訊、資通系統，建立資產目錄。 本校依資通安全責任等級分級辦法，為責任等級 D 級機關。
6. 資通安全風險評估	6.1 資通安全風險評估	本校已於今年 01 月完成本校之資訊、資通系統及相關資產之風險分析評估及處理。
	6.2 資通安全風險之因應	本校已依資通安全風險評估之結果擬定對應之資通安全防護及控制措施。
7. 資通安全防護及控制措施	7.1 資訊及通系統之保管	本校已依安全維護計畫辦理，詳附件資料。
	7.2 存取控制與加密機制管理	本校已依安全維護計畫辦理。
	7.3 作業及通訊安全管理	本校已依安全維護計畫辦理。
	7.4 系統獲取、開發及維護	本校已依安全維護計畫辦理。
	7.5 執行資通安全健診	本校已依安全維護計畫辦理。
8. 資通安全事件通報、應變及演練相關機制	8.1 訂定資通安全事件通報、應變及演練相關機制	本校已依規定訂定資通安全事件通報應變程序。(詳附件)

	8.2 資通安全事件通報、應變及演練	本校已依規定進行資通安全事件通報，每年9月辦理通報應變演練。
9. 資通安全情資之評估及因應機制	9.1 資通安全情資之分類評估	本校接受情資後，已進行分類評估。
	9.2 資通安全情資之因應措施	本校已接受情資之分類，採取對應之因應措施。
10. 資通系統或服務委外辦理之管理	10.1 選任受託者應注意事項	本校資通系統或服務委外辦理時，已將選任受託者應注意事項加入招標文件中。
	10.2 監督受託者資通安全維護情形應注意事項	本校已依規定監督受託者資通安全維護情形，客製他資通系統開發者，已要求其出具安全性檢測證明。
11. 資通安全教育訓練	11.1 資通安全教育訓練要求	本校人員已規定進行資通安全教育訓練。
	11.2 辦理資通安全教育訓練	本校已於今年1月辦理資通安全教育訓練。
12. 公務機關所屬人員辦理業務涉及資通安全事項之考核機制	12.1 訂定考核機制並進行考核	本校已建立考核機制，並已依規定進行平時及年終考核。

13. 資通安全維護計畫及實施情形之持續精進及績效管理機制	13.1 資通安全維護計畫之實施	本校已依規定訂定各階文件、流程、程序或控制措施，據以實施並保存相關之執行成果記錄。
	13.2 資通安全維護計畫實施情形之稽核機制	本校已依規定辦理內部稽核。
	13.3 資通安全維護計畫之持續精進及績效管理	本校已依規定辦理內部召開管理審查會議，確認資通安全維護計畫之實施情形，確保其持續適切性、合宜性及有效性。
其他說明		

業務承辦人：

單位主管：

資通安全長：

臺北市北投區石牌國民小學資通安全稽核計畫

壹、依據：

- 一、本校資通安全維護計畫辦理。
- 二、資通安全管理法第十三條規定辦

理。貳、目的：

為瞭解本校資通安全維護計畫執行之有效性，爰擬定本稽核計畫，執行稽核作業。

參、稽核期程：

於每年 10 月前召開資通安全管理審查會議進行稽

核。肆、稽核團隊成員：

資通安全長及各單位主管兼任。

伍、稽核範圍：

全校。

陸、稽核項目及內容：

依據本校安全維護之內容，本年度之稽核項目、內容如下：

- 一、核心業務及其重要性盤點：詳參本校資通安全維護計畫，下同。
- 二、資通安全政策及目標：資安政策宣導及定期召開資安管理會議。
- 三、資通安全推動組織。
- 四、人力及經費之配置。
- 五、學校資通安全長之配置。
- 六、資訊及資通系統之盤點，並標示核心資通系統及相關資產，建立資產目錄。

七、資通安全風險評估。

八、資通安全防護及控制措施。

九、資通安全事件通報、應變及演練相關機制。十、

資通安全情資之評估及因應機制。

十一、資通系統或服務委外辦理之管理措施。

十二、公務機關所屬人員辦理業務涉及資通安全事項之考核機制。

十三、資通安全維護計畫及實施情形之持續精進及績效管理機制。

柒、改善作業

本校經評估對於稽核結果表現優良者依公務機關所屬人員資通安全事項獎懲辦法給予行政獎勵，並針對缺失或待改善項目者研擬後續追蹤方式及頻率（如將前次稽核結果納入本次稽核範圍中，並追蹤辦理情形及進度）。

捌、實施

本計畫由校長核可後實施，修改時亦同。

16. 稽核項目紀錄表

臺北市北投區石牌國民小學稽核項目紀錄表

稽核日期： 年 月 日稽核範圍：全校

受稽核單位	稽核項目	稽核結果	備註
		<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
		<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
		<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
		<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
		<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
		<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
附註			
受稽核人員：			受稽核單位主管：

17. 稽核委員聘任同意暨保密切結書

臺北市北投區石牌國民小學資訊安全工作稽核委員聘任同意暨保密切結書

本人（以下簡稱甲方）為協助臺北市北投區石牌國民小學（以下簡稱乙方）執行「資訊安全稽核工作」（以下簡稱本計畫），接受乙方之邀請，擔任 112 年資安稽核團隊之稽核委員，特立書同意事項如下：

一、 甲方應遵守國家機密保護法、個人資料保護法、行政院及所屬各機關資訊安全管理要點、行政院及所屬各機關資訊安全管理規範、著作權法及其他相關法令之規定，並對因執行本計畫或因執行本計畫之機會所知悉之機密資訊負有保密義務；且上開各義務不因甲方與乙方或與技服中心間，就本年度擔任稽核委員相關事宜之法律關係解除、終止或完成而失其效力。

二、 甲方就因執行本計畫或因執行本計畫之機會，所知悉或接觸之乙方、受稽機關或其他第三人之機密資訊，除因執行本計畫所必須，且事先經乙方書面同意者，或法律另有明文規定外，不得有下列行為：

- (一) 全部或一部重製或留存上開機密資訊；
- (二) 以任何方式向任何第三人揭露上開機密資訊之全部或一部；
- (三) 以任何方式使任何第三人知悉、持有或使用上開機密資訊之全部或一部；
- (四) 以任何方式使自己或任何第三人就上開機密資訊之全部或一部取得任何權利；
- (五) 揭露、公開或使用上開機密資訊之全部或一部。

三、 甲方因執行本計畫所製作之報告、文件或其他產出，其智慧財產權及其他權利均歸屬乙方所有。

四、 甲方與受稽機關有下列情形之一者，就與該受稽機關之稽核相關事宜，應主動迴避，或事先以書面告知乙方，以確認是否得免予迴避：

- (一) 甲方、甲方之配偶、甲方三親等以內血親或姻親、與甲方有共同生活關係之家屬、或上開人員財產信託之受託人，與受稽機關間，有財產上或非財產上利益之利害關係者；
- (二) 甲方、甲方之配偶、甲方三親等以內血親或姻親、與甲方有共同生活關係之家屬，與受稽機關或其負責人間現有或於過去兩年間曾有僱傭、承攬、委任、代理或其他類似之關係者；

(三) 甲方或其現任職或於過去兩年內曾任職之機關，於民國 112 年至本次稽核期間，曾為受稽機關進行與受稽事項相關之顧問輔導者。

五、前條所稱財產上利益，係指動產、不動產、現金、有價證券、債權、其他財產上權利、具有經濟價值或得以金錢交易取得之利益；所稱非財產上利益，係指有利於甲方之配偶、甲方三親等以內血親或姻親、與甲方有共同生活關係之家屬、或上開人員財產信託之受託人於受稽機關或其關聯機關之任用、陞遷、調動及其他人事措施。

六、有其他情形足認甲方有不能公正執行職務之虞，經受稽機關敘明理由，並由乙方作成迴避決定者，甲方應迴避之。

七、甲方有第四條各款情形之一，而未自行迴避，亦未事先以書面告知乙方相關情事，並經乙方書面同意免予迴避者，乙方得終止本契約，甲方應返還已收取之報酬，如乙方，因此認有必要對受稽機關重為全部或一部稽核，或受有其他不利益時，甲方並應賠償乙方因此所生之一切損失及費用（包括但不限於賠償金、和解金、律師費及訴訟費用等）。

八、甲方如違反第二條或就相關事宜涉及其他不法情事，將移送司法機關處理；如致乙方、受稽機關，遭受任何不利益，或受第三人法律上請求或訴追者，甲方應賠償乙方、受稽機關，因此所生之一切損失及費用（包括但不限於賠償金、和解金、律師費及訴訟費用等）。

九、甲方應公正執行職務，並應避免使人誤認推薦特定廠商、產品或服務；且處理稽核相關事務或出席會議，應親自為之。

此 致

臺北市北投區石牌國民小學

立 同 意 書 人

姓 名：

（簽章）身 份 證 字 號：

中 華 民 國 年 月 日

臺北市北投區石牌國民小學稽核結果及改善報告

稽核範圍				
稽核日期				
審查日期				
改善措施				
編號	稽核缺失或待改善稽核項目	改善措施	改善期程規劃	相關證明資料
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				

業務承辦人：

單位主管：

資通安全長：

19.改善績效追蹤報告

臺北市北投區石牌國民小學改善績效追蹤報告

編號：

製表日期：

稽核發現			
稽核日期		受稽核單位	
稽核區域			
缺失或待改善項目與內容			
影響範圍評估			
發生原因分析			
改善措施成效追蹤			
改善措施		預計成效	執行情況
管理面			

技術面			
人力面			
資源面			
作業程序			
其他			

績效管考			
改善措施確認			
經費需求 或編列執行金額		經費執行情形	
預定完成日期		實際完成日期	
完成進度或情形說明			
改善成效考核			
後續成效追蹤			
業務承辦人		資通安全長	

附件四：修正本校性騷擾防治措施、申訴及規範一件附件

臺北市北投區石牌國民小學性騷擾防治措施、申訴及懲戒規範修正條文對照表

修正條文	現行條文	說明
二十四、本規範由校務會議通過後公告實施，修正時亦同。	二十四、本規範由校長奉核公佈後實施，修訂時亦同。	一、依臺北市政府教育局 114 年 11 月 7 日北市教人字第 1143112221 號函略以，各級學校依據性騷擾防治法第 7 條及性別平等工作法第 13 條訂定性騷擾防治措施（包含三法整合之處理機制）等校內章則，均屬校務重大事項，應提交校務會議議決。 二、修正本條程序，並酌作文字修正。

臺北市北投區石牌國民小學性騷擾防治措施、申訴及懲戒規範修正草案

107.04.02 訂定

111.12.08 修正

112.07.06 修正

112.09.23 修正

113.03.06 修正

113.06.18 修正

114.03.21 修正

一、臺北市北投區石牌國民小學（以下簡稱本校）為提供所屬人員、求職者或受服務人員免於性騷擾之工作及受服務環境，並採取適當之預防、糾正、懲戒及處理措施，以維護當事人權益及隱私，特依性別平等工作法第 13 條第 1 項、勞動部頒布「工作場所性騷擾防治措施準則」及性騷擾防治法第 7 條第 1 項、第 2 項規定，訂定本規範。

二、本規範適用於所屬人員、求職者或受服務人員遭遇前揭適用性別平等工作法或性騷擾防治法之性騷擾事件，但應適用性別平等教育法處理者，不適用本規範。

三、本規範所稱之性騷擾，指當事人有下列情形之一者：

（一）適用性別平等工作法：

1.指所屬人員（含受僱者、派遣勞工、技術生及實習生）於執行職務時，任何人（含雇主、各級主管、員工、客戶…等）以性要求、具有性意味或性別歧視之言詞或行為，對其造成敵意性、脅迫性或冒犯性之工作環境，致侵犯或干擾其人格尊嚴、人身自由或影響其工作表現。

2.雇主對所屬人員（含受僱者、派遣勞工、技術生及實習生）或求職者為明示或暗示之性要求、具有性意味或性別歧視之言詞或行為，作為勞務契約成立、存續、變更或分發、配置、報酬、考績、陞遷、降調、獎懲之交換條件。

3.性別平等工作法所稱權勢性騷擾，指對於因僱用、求職或執行職務關係受自己指揮、監督之人，利用權勢或機會為性騷擾。

4.有下列情形之一者，適用本規範之規定：

(1)本校所屬人員於非工作時間，遭受所屬事業單位之同一人，為持續性性騷擾。

(2)本校所屬人員於非工作時間，遭受不同事業單位，具共同作業或業務往來關係之同一人，為持續性性騷擾。

(3)本校所屬人員於非工作時間，遭受最高負責人或僱用人為性騷擾。

（二）適用性騷擾防治法：

1.除性侵害犯罪以外（性侵害犯罪部分，除申訴程序外，準用本規範相關規定），對他人實施違反其意願而與性或性別有關之行為，且有下列情形之一者：

(1)以明示或暗示之方式，或以歧視、侮辱之言行，或以他法，而有損害他人人格尊嚴，或造成使人心生畏怖、感受敵意或冒犯之情境，或不當影響其工作、教育、訓練、服務、計畫、活動或正常生活之進行。

(2)以該他人順服或拒絕該行為，作為自己或他人獲得、喪失或減損其學習、工作、訓練、服務、計畫、活動有關權益之條件。

2.性騷擾防治法所稱權勢性騷擾，指對於因教育、訓練、醫療、公務、業務、求職或其他相類關係受自己監督、照護、指導之人，利用權勢或機會為性騷擾。

性騷擾之樣態，包含下列行為之一：

- (一) 羞辱、貶抑、敵意或騷擾之言詞或行為。
- (二) 跟蹤、觀察，或不受歡迎之追求。
- (三) 偷窺、偷拍。
- (四) 曝露身體隱私部位。
- (五) 以電話、傳真、電子通訊、網際網路或其他設備，展示、傳送或傳閱猥褻文字、聲音、圖畫、照片或影像資料。
- (六) 乘人不及抗拒親吻、擁抱或觸摸臀部、胸部或其他身體隱私部位。
- (七) 其他與前六款相類之行為。

四、性騷擾之調查除依性別平等工作法第 12 條第 1 項至第 4 項規定認定外，並得綜合審酌下列各款情形：

- (一) 不適當之凝視、觸摸、擁抱、親吻、嗅聞他人身體任何部位；強行使他人對自己身體任何部位為之，亦同。
- (二) 寄送、留置、展示或播送性要求、具有性意味或性別歧視之文字、圖畫、聲音、影像或其他物品。
- (三) 反覆或持續違反意願之跟隨或追求行為。

五、本校應防治性騷擾之發生，消除工作或服務場所內源自於性或性別的敵意因素，以保護所屬人

員、求職者及受服務人員不受性騷擾之威脅。如有性騷擾或疑似情事發生時，應即檢討、改善防治措施。另針對所屬人員於非雇主所能支配、管理之工作場所工作者，雇主應為工作環境性騷擾風險類型辨識、提供必要防護措施，並事前詳為告知。

六、本校應妥適利用集會、公告、電子郵件或內部文件等各種傳遞訊息之機會與方式，加強對所屬員工有關性騷擾防治措施及申訴管道之宣導。

本校就下列人員，實施防治性騷擾之教育訓練：

- (一) 員工應接受工作場所性騷擾防治之教育訓練。
- (二) 擔任主管職務以及參與性騷擾申訴事件之處理、調查及決議人員，每年應定期接受相關教育訓練。

前項教育訓練，本校性騷擾專責處理人員及擔任主管職務者，優先實施。

七、本校性騷擾申訴管道如下：

申訴專線電話：(02)28227484 分機 661、662

申訴專用傳真：(02)28209860

申訴專用信箱或申訴電子信箱：79400y@tp.edu.tw

專責處理人員姓名或單位名稱：人事室

本校校長涉及「性別平等工作法」之性騷擾事件者，申訴人應向臺北市政府教育局提出申訴；涉及「性騷擾防治法」之性騷擾事件者，申訴人應依「性騷擾防治法」第 14 條規定向臺北市政府社會局提出，其處理程序依各該主管機關規定辦理。

涉及「性騷擾防治法」案件，申訴時行為人不明或非本校所屬教職員工：向性騷擾事件發生地之警察機關提出。

八、本校於知悉性騷擾之情形時，應採取下列立即有效之糾正及補救措施，並注意被害人安全及隱私之維護；被害人及行為人分屬不同事業單位，且具共同作業或業務往來關係者，該行為人之雇主，亦同：

（一）因接獲被害人申訴而知悉性騷擾之情形時：

1. 考量申訴人意願，採取適當之隔離措施，避免申訴人受性騷擾情形再度發生，並不得對申訴人工作條件作不利之變更。
2. 對申訴人提供或轉介諮詢、醫療或心理諮商、社會福利資源及其他必要之服務。
3. 對身心障礙者依其障別提供必要之協助。
4. 協助申訴人保留相關證據，啟動調查程序，對性騷擾事件之相關人員進行訪談或適當之調查程序。
5. 被申訴人具權勢地位，且情節重大，於進行調查期間有先行停止或調整職務之必要時，得暫時停止或調整被申訴人之職務；經調查未認定為性騷擾者，停止職務期間之薪資，應予補發。
6. 本校校長或各級主管涉及性騷擾行為，且情節重大，於進行調查期間，校長得由臺北市政府教育局、各級主管得由本校先行停止或調整職務。但其他法律別有規定者，從其規定。其案件調查結果未經認定為性騷擾，或經認定為性騷擾但未依公務人員、教育人員或其他相關法律予以停職、免職、解聘、停聘或不續聘者，得依各該法律規定申請復職，及補發停職期間之本俸（薪）、年功俸（薪）或相當之給與。
7. 性騷擾行為經查證屬實，將視情節輕重對行為人為適當之懲處或處理。
8. 如經證實有惡意虛構之事實者，亦對申訴人為適當之懲戒或處理。

（二）非因前款情形而知悉性騷擾事件時：

1. 就相關事實進行必要之釐清。
2. 依被害人意願，協助其提起申訴。
3. 適度調整工作內容或工作場所。
4. 依被害人意願，提供或轉介諮詢、醫療或心理諮商處理、社會福利資源及其他必要之服務。

本校於所屬公共場所及公眾得出入之場所，為有效預防並積極處理性騷擾事件，應有如下作為：

- （一）就所屬公共場所及公眾得出入之場所，定期檢討其空間及設施，避免性騷擾之發生。

(二) 於所屬公共場所及公眾得出入之場所發生有性騷擾事件當時知悉者，應採取下列有效之糾正及補救措施：

- 1.注意被害人安全。尊重被害人意願，減低當事人互動之機會，預防、減低行為人再度性騷擾之可能。避免報復情事。
- 2.注意被害人隱私之維護。
- 3.協助被害人申訴及保全相關證據。
- 4.必要時協助通知警察機關到場處理。
- 5.檢討所屬場所安全。
- 6.其他認為必要之處置。

(三) 於性騷擾事件發生後知悉者，仍應採取有效糾正補救措施再次檢討所屬場所安全。

九、性騷擾之申訴得以言詞、電子郵件或書面提出。以言詞或電子郵件為申訴者，受理之人員或單位應作成紀錄，經向申訴人朗讀或使閱覽，確認其內容無誤後，由其簽名或蓋章，確認其內容無誤。

申訴書應載明事項：

(一) 申訴人之姓名、性別、年齡、身分證統一編號或護照號碼、服務、工作或就學之單位及職稱、住所或居所、聯絡電話。

(二) 有法定代理人者，其姓名、性別、年齡、身分證統一編號或護照號碼、職業、住所或居所、聯絡電話。

(三) 有委任代理人者，應檢附委任書，並載明其姓名、性別、年齡、身分證統一編號或護照號碼、職業、住所或居所、聯絡電話。

(四) 申訴之事實內容及可取得之相關證據。

(五) 性騷擾事件發生及知悉之時間。

(六) 申訴之年月日。

適用性騷擾防治法事件之申訴，申訴書或言詞作成之紀錄不合前項規定，而其情形可補正者，應通

知申訴人於 14 日內補正。逾期未補正者，本校應即移送臺北市政府處理。

本校依性別平等工作法之工作場所性騷擾預防、糾正及補救義務，不因申訴不受理而受影響。

十、本校教職員工生違反性騷擾防治法而由本校調查處理時，其處理程序如下：

(一) 性騷擾申訴如應適用性別平等教育法或性別平等工作法性騷擾事件，應於接獲之日起 20 日內，移送該事件之主管機關，並副知當事人。

(二) 性騷擾申訴案件如於本校不具調查權限者，應於接獲申訴之日起 14 日內查明並移送具有調查權之受理單位，未能查明調查單位者，應移送性騷擾事件發生地之警察機關就性騷擾申訴為調查。移送時以書面通知當事人，並副知臺北市政府。

(三) 有下列情事應不予受理者，移送臺北市政府決定不予受理或應續行調查：

1. 當事人逾期提出申訴。
2. 申訴不合法定程式，經通知限期補正，屆期未補正。
3. 同一性騷擾事件，撤回申訴或視為撤回申訴後再行申訴。

(四) 確認受理之申訴案件，應於受理申訴或移送到達之日起 7 日內進行調查，並於 2 個月內調查完畢，必要時得延長 1 個月，延長以 1 次為限，並通知當事人。

(五) 調查完畢後本校應作成調查報告及處理建議，移送臺北市政府審議。

十一、本校雖非行為人所屬單位，於接獲本規範第 3 條第 2 款之性騷擾申訴書時，仍應採取適當之緊急處理，並應於 7 日內將申訴書及相關資料移送臺北市政府社會局。

十二、本校為處理性騷擾申訴案件，應設性騷擾申訴處理單位（即性騷擾申訴處理調查會，以下簡稱申調會），組成委員人數 6 人，其中應有具備性別意識之專業人士，且女性成員比例不得低於二分之一；其成員至少應有三分之二為「外部」專家學者，並應組成「申訴調查小組」，負責申訴案件之調查（含相關人員訪談、紀錄等）、調查報告撰擬及研提處理建議等，調查完成後應將調查結果移送申訴處理單位審議處理；該小組成員不得由本校人員擔任，且至少應有三分之二為具備性別意識之外部專家學者。

十三、針對適用性別平等工作法之派遣勞工如於執行勤務時遭受性騷擾事件，本校將受理申訴，並與派遣事業單位共同調查，且將調查結果通知派遣事業單位及當事人。

十四、申調會作成決議前，得由申訴人或其授權代理人以書面撤回其申訴；申訴經撤回者，不得就同一事由再為申訴。

前項情形於性騷擾防治法事件之申訴，除經主管機關調解成立且撤回申訴者外，不在此限。

十五、申調會應有委員半數以上出席始得開會，並應有半數以上之出席委員之同意始得做成決議，可否同數時取決於主席。

委員會召開會議時，得通知當事人及關係人到場說明，給予當事人充分陳述意見及答辯機會，除有詢問當事人之必要外，應避免重複詢問，並得邀請具相關學識經驗者協助。

十六、參與性騷擾事件之處理、調查及決議人員，應對於知悉之申訴事件內容應予保密。違反者，主任委員終止其參與，本校並得視其情節依相關規定予以懲處及追究相關責任，並解除其聘任。

十七、性騷擾事件之處理，有下列情形之一者，處理、調查與決議人員應自行迴避：

- (一) 本人或其配偶、前配偶、四親等內之血親或三親等內之姻親或曾有此關係者為事件之當事人時。
- (二) 本人或其配偶、前配偶就該事件與當事人有共同權利人或共同義務人之關係者。
- (三) 現為或曾為該事件當事人之代理人、輔佐人者。
- (四) 於該事件，曾為證人、鑑定人者。

性騷擾事件申訴之處理、調查與決議人員有下列情形之一者，當事人得申請迴避：

- (一) 有前項所定之情形而不自行迴避者。

(二) 有具體事實，足認其執行調查有偏頗之虞者。

前項申請，應舉其原因及事實，向申調會為之，並應為適當之釋明；被申請迴避之調查人員，對於該申請得提出意見書。

被申請迴避之調查人員在申調會就該申請事件為準駁前，應停止調查工作。但有急迫情形，仍應為必要處置。

處理、調查與決議人員有第一項所定情形不自行迴避，而未經當事人申請迴避者，應由該申調會命其迴避。

十八、本校申訴調查小組調查性騷擾事件時，應依照下列調查原則為之：

(一) 性騷擾事件之調查，應以不公開之方式為之，並保護當事人之隱私及人格法益。

(二) 性騷擾事件之調查應秉持客觀、公正、專業原則，給予當事人充分陳述意見及答辯之機會。

(三) 被害人之陳述明確，已無詢問必要者，應避免重複詢問。

(四) 性騷擾事件之調查，得通知當事人及關係人到場說明，並得邀請相關學識經驗者協助。

(五) 性騷擾事件之處理，應避免當事人或證人對質。

(六) 調查人員因調查之必要，得於不違反保密義務範圍內另作成書面資料，交由當事人閱覽或告以要旨。

(七) 處理性騷擾事件之所有人員，對於當事人之姓名或其他足以辨識身份之資料，除有調查必要或基於公共安全之考量者外，應予保密。

(八) 性騷擾事件調查過程中，得視當事人之身心狀況，主動轉介或提供心理輔導及醫療與法律協助。

(九) 對於在性騷擾事件申訴、調查、偵察或審理程序中，為申訴、告訴、告發、提起訴訟、作證、提供協助或其他參與行為之人，不得為不當之差別待遇。

(十) 性騷擾事件之調查人員應具備性別平等意識。

十九、申調會應於申訴提出或移送申訴案件到達之日起 7 日內開始調查，並應自接獲或受理性騷擾申訴之翌日起 2 個月內結案；必要時，得延長 1 個月，並通知當事人。

二十、調查結果通知及救濟途徑：

(一) 適用性別平等工作法：申調會之調查結果，應作成附理由之決議，並得作成懲處或其他處理之建議。該調查決議應以書面通知雙方當事人及本校，並註明對申訴案之決議有異議者，依下列法令得提出之救濟途徑：

1. 當事人屬「公務人員保障法」之適(準)用對象者，得依「公務人員保障法」規定提起復審。
2. 當事人非屬「公務人員保障法」之適(準)用對象者，得依「性別平等工作法」第 32 條之 1 第 1 項第 2 款規定，於提起申訴之期限內向地方主管機關提起申訴。

(二) 適用性騷擾防治法：本校應將調查報告及處理建議移送臺北市政府審議，經審議後，由臺北市政府將該申訴案件之調查結果通知當事人及本校。當事人如不服臺北市政府之申訴調查結果，得於調查結果通知送達之次日起 30 日內檢附行政處分影本、訴願書至臺北市政府，由臺北市政府層轉訴願管轄機關即衛生福利部審議，如不服訴願決定，得於決定書送達之次日起 2 個月內提起行政訴訟。

二十一、性騷擾行為經調查屬實且已結案者，本校得視情節輕重，對受僱之行為人按其身分適用法規給予懲處，並應循法定程序於一週內啟動行政懲處作業，懲處額度依本府規定應核予「記過」以上之處分，當年度考績(成、核)應考列「丙等」或依其適用法規之相當等次；適(準)用公務人員陞遷法者，另依該法第 12 條第 1 項第 6 款「最近一年內對他人為性騷擾或跟蹤騷擾，致平時考核曾受記過一次以上之處分」之規定，不得辦理陞任。如涉及刑事責任時，本校並應協助申訴人提出告訴或告發。性騷擾行為經證實為誣告者，本校得視情節輕重，對申訴人為適當之懲處或處理。

本校依性別平等工作法第 27 條第 1 項及第 2 項與性騷擾行為人連帶負損害賠償責任時，於本校賠償被害人損害後，對於性騷擾行為人，有求償權。

二十二、本校對性騷擾事件之決議及處理應採取追蹤、考核及監督，以確保懲戒或處理措施有效執

行，並避免相同事件或報復情事發生。

二十三、本校不會因所屬人員提出本規範所訂之申訴或協助他人申訴，而予以解僱、調職或其他不利處分。

二十四、本規範由校務會議通過後公告實施，修正時亦同。

臺北市政府教育局 函

地址：110204臺北市信義區市府路1號8樓
承辦人：簡建雄
電話：02-27208889轉6405
傳真：02-27205627
電子信箱：be6320@gov.taipei



受文者：臺北市北投區石牌國民小學

發文日期：中華民國114年11月7日
發文字號：北市教人字第1143112221號
速別：普通件
密等及解密條件或保密期限：
附件：教育部書函影本1份 (40169395_1143112221_1_ATTACHMENT1.pdf)

主旨：重申各級學校依據性騷擾防治法第7條及性別平等工作法第13條訂定性騷擾防治措施（包含三法整合之處理機制）等校內章則，均屬校務重大事項，應提交校務會議議決一案，請查照。

說明：

- 一、依教育部101年9月26日臺訓（三）字第1010156729號書函略以，國民教育法第10條（現為第19條）、高級中學法第23條（現為高級中等教育法第25條）、職業學校法第10條之5（現為高級中等教育法第25條）、大學法第15條及第16條第2款、專科學校法第19條及第20條第2款（現分別為第21條及第22條第2款），均定有「設校務會議，議決校務重大事項」之規定，學校防治性侵害、性騷擾及性霸凌事件之發生，其工作要項包括空間安全之規劃檢視與檢討改善、人員（教職員工生）之教育宣導與人際互動之約束，



及該等事件之處理機制及危機管理之分工等，屬校務重大事項殆無疑義。爰學校依據旨揭法律所制定之章則，應請提交校務會議議決。

二、復經本局洽教育部確認，旨揭性騷擾防治措施等校內章則修正案亦屬校務重大事項，爰亦應提交校務會議議決，併予敘明。

三、邇來本局屢接獲民眾陳情，部分學校於修訂性騷擾防治措施時，未依前揭教育部函釋規定提交校務會議議決，爰重申規定，請各校務必重行審視修訂程序是否符合前開教育部書函規定，如未依規定將性騷擾防治措施提交校務會議議決者，應儘速補行提交確認。

四、檢附教育部101年9月26日書函影本1份。

正本：臺北市立大學、臺北市政府教育局所屬公立各級學校、臺北市各市立幼兒園

副本：

2025/11/10
10:44:46
電子文件
交換章