臺北市立龍門國民中學資訊安全須知

1. 資訊設施之存取應與本身業務相關範圍為主，任何人未經授權不得存取業務範圍外之資訊設施。

2. 應正確地使用資訊設施，以維護設施的可用性、完整性與機密性。

3. 非因業務需求不得將系統存取帳號提供給外部人員，若因業務需要開放帳號予外部人員，應有適當安全控管措施，該安控措施應考量業務需求及資訊資產之機密性，授與適當之存取權限及有效日期。

4. 因處理系統當機與異常狀況需視狀況授與適當存取權限，並由資訊系統管理者陪同處理之。

5. 可攜帶式電腦儲存媒體，例如：筆記型電腦、隨身碟、光碟、磁帶等，應採取適當管控措施，防止未經授權資料、系統、網路存取或病毒傳播。

6. 資料、資訊之存取，必須符合「電腦處理個人資料保護法」、「電子簽章法」及「智慧財產權」等相關法規之法令規定，或契約對資料保護及資料存取使用管控之權責規定。

7. 業務資料或程式之存取權限應適當控管，禁止未受權者存取。

8. 針對無人看管的資訊資產設備，應有適當控管程序，以防經未授權之存取或濫用。

9. 個人桌上型電腦、可攜式電腦應設定於一定時間不使用或離開後，應自動清除螢幕上的資訊並登出或鎖定系統，以避免被未授權之存取。

10. 新購置之應用軟體或系統，安裝完成後應立即更新預設之密碼，並刪除或關閉不必要之帳號。

11. 欲使用網路硬碟者請填寫「網路硬碟申請表」，由帳號管理人員進行使用者帳號建立作業。

12. 系統管理者應避免共用系統管理者帳號，系統管理者帳號與密碼應存放於安全之處。

13. 系統管理者密碼設置，至少8 碼，且應符合密碼設置原則(密碼應同時包含英文字母及數字)。

14. 使用者首次使用系統時，應立即更改密碼設定，並妥善保管帳號與維持密碼之機密性，保存帳號密碼之檔案應以加密方式處理。

15. 使用者應避免將帳號密碼記錄在書面上，張貼在個人電腦、螢幕或其他容易洩漏秘密之場所。

16. 使用者發現密碼可能遭破解時，應立即更改密碼。

17. 使用者每次存取系統時應輸入密碼登入系統，避免使用記錄密碼功能自動登入系統之功能。

18. 使用者密碼設置至少6 碼，且應符合密碼設置原則。

19. 應儘量避免使用易猜測或公開資訊為設定，例如：個人姓名、出生年月日、身分證字號、機關、單位名稱或其他相關事項、使用者ID、其他系統ID、電腦主機名稱、作業系統名稱、電話號碼、空白、字典字彙等。

20. 密碼設定可考慮下列原則：

參雜數字、英文字母、特殊符號、大小寫、不易忘記特殊意義詞彙。

21. 使用者遺忘密碼時，須填具「資訊服務申請單」，經單位主管核准後，由帳號管理人員重新設定。

22. 遇到他人以任何身份要求個人或公司資料時，應先謹慎確認身份。

23. 不管是信件或言詞交談，應小心勿隨意透露重要資訊給他人。

24. 勿用電子郵件內提供的超連結，以自己輸入網址方式取代。

25. 收到要求輸入個人資料的電子郵件時，一定要和原公司求證，以減少被騙機會。

26. 不開啟任何來路不明的磁片、光碟、email 的附加檔，尤其是不認識的人寄來的電子郵件附加檔。

27. 電腦要安裝防毒軟體，病毒碼也要時時更新。

28. cookie 紀錄重要的個人資料與網路使用習慣，應隨手刪除電腦裡的cookie 紀錄。

29. 詳讀每個網站的隱私權政策，尤其是cookie 所蒐集的使用者資訊用途，以避免個人資料被濫用。

30. 使用網路交易或者填寫個人資料時，需先檢查該網站是否有安全認證標章。

31. 使用網路購物或網路銀行時，應檢查網址列開頭是否為https，以確保資料傳輸有加密安全機制。