

資訊科技教育計劃

學校

資訊科技保安

香港特別行政區政府
教育局
教育基建分部

www.edb.gov.hk/ited/

二零零七年五月修訂

如就本文件有任何問題，請致電(852) 3698 3608向教育局資訊科技教育組查詢；
或致函九龍九龍塘沙福道19號教育局九龍塘教育服務中心東座420室教育基建分部
資訊科技教育組總課程發展主任收。

本刊物全文刊載於資訊科技教育網站：<http://www.edb.gov.hk/ited/>。

目錄

1	為何資訊科技保安對學校如此重要？	1
2	保安基礎	3
2.1	資訊科技保安目標	3
2.1.1	機密性	3
2.1.2	完整性	3
2.1.3	可用性	3
2.2	資訊科技保安監控	3
2.2.1	實體保安	4
2.2.2	接達控制	4
2.2.3	數據保安	4
2.2.4	網絡和通訊保安	4
2.2.5	保安審查和事故處理	5
2.2.6	用戶關注及教育	5
2.2.7	其他保安問題	5
2.3	權衡利弊	5
2.4	更多資訊	5
3	實體保安	7
3.1	安全區劃分	7
3.2	硬件及軟件資產保護	7
3.2.1	進出媒體	7
3.2.2	伺服器室保安	8
3.2.3	樓層設備櫃的保安	8
3.2.4	電源受損防護	8
3.2.5	流動裝置	8
3.2.6	儲存媒體	8
3.2.7	軟件備份及備份帶	8
3.2.8	保安標記及設備清單	8
3.3	更多資訊	9
4	接達控制	10
4.1	賬戶管理	10
4.1.1	普通賬戶	10
4.1.2	特殊賬戶	11
4.2	用戶保安選項	12
4.2.1	密碼處理	12
4.2.2	用戶及使用權限設定	13
4.3	更多資訊	14
5	數據保安	15
5.1	資料分類	15
5.2	資料處理	15
5.2.1	儲存於伺服器的資料	16
5.2.2	資料備份及復原	16
5.2.3	儲存媒體的標籤及貯存	16

5.2.4	敏感資料的保護及棄置	16
5.2.5	保護個人資料的原則	17
5.3	預防電腦病毒	17
5.3.1	防毒軟件	17
5.3.2	合法及經授權使用的軟件和硬件	17
5.3.3	遠離可疑檔案資源	18
5.3.4	用戶教育及事故處理	18
5.4	軟件配置及更改監控	18
5.4.1	關閉或刪除所有不必要的服務及組件	18
5.4.2	使用管理工具	19
5.4.3	應用備受推薦的保安漏洞修正方案	19
5.5	更多資訊	20
6	網絡和通訊保安	22
6.1	學校與外界網絡之間的通訊	22
6.1.1	遙距接達	22
6.1.2	接達互聯網	23
6.2	學校的局部區域網絡	28
6.2.1	相同保安級別的局部區域網絡	28
6.2.2	不同保安級別的局部區域網絡	29
6.3	對濫發電郵及惡意程式的防護	31
6.3.1	濫發電郵	31
6.3.2	惡意程式	32
6.4	網絡應用系統保安	32
6.4.1	網絡應用系統保安結構	32
6.4.2	網絡應用系統開發程序	33
6.5	更多資訊	34
7	保安審查及保安事故處理	35
7.1	保安審查	35
7.2	保安事故處理程序	35
7.2.1	例子－處理病毒感染	36
7.2.2	例子－處理網絡入侵	37
7.3	更多資訊	40
8	用戶關注及教育	41
8.1	教育至為重要！	41
8.2	保護電腦及用戶	41
8.2.1	例子－用戶在互聯網上的安全	41
8.2.2	互聯網上的風險	41
8.2.3	教育及指引	42
8.3	最佳安排	42
8.3.1	教育方法	42
8.3.2	義務及責任	42
8.3.3	推廣及督導	43
8.4	更多資訊	43
9	資訊科技保安政策	45
9.1	甚麼是資訊科技保安政策？	45

9.1.1	擬定政策	45
9.1.2	系統配合	45
9.1.3	教育及推廣	45
9.1.4	審查及檢討	46
9.2	更多資訊.....	46
10	結語	47

1 為何資訊科技保安對學校如此重要？

目前，香港大部分學校已經安裝了本身的局部區域網絡（LAN），如網上校管系統（WebSAMS）、學校學與教網絡，以及設於部分學校的多媒體學習中心（MMLC）等。

為提高學與教質素以及擴闊接達資訊的渠道，大部分學校已獲得上網服務，有些學校甚至將學校網頁寄存在互聯網服務供應商（ISP）裡。部分學校亦開拓新的資訊科技工具，例如設立學校內聯網系統，讓教師及學生互動交流及進行協作。

據我們估計，倘若學校的資訊科技設施不能正常運作或數據無法存取，學校的營運將會受到不良的影響。

簡介

本文件提供的資訊科技保安基礎知識及概念，適用於學校的環境。本文件概括地介紹了學校在制定資訊科技保安政策時須考慮的目的或目標，以及在每個資訊科技保安監控範圍內的重要問題。

本文件旨在協助學校因應本身情況釐定適合的校本資訊科技保安政策及標準。

本文件專為學校所有資訊科技用戶而設，包括學校資訊科技管理層、技術員以及終端用戶。資訊科技管理層，例如校長、資訊科技統籌員、學校資訊科技委員會成員，會發現文件提供的資訊對於他們釐定高層次的校本資訊科技保安政策有極大幫助。技術員，例如局部區域網絡管理員及其他技術支援人員，可以本文件為基礎，制訂適用於學校環境的詳細資訊科技保安指引及標準。文件中的部分資訊亦會對終端用戶，包括有使用資訊科技設施的學生、教師及其他職員，或甚至家長等，有一定的參考價值，旨在提高他們對使用資訊科技設施的安全意識。

在電腦系統內，存在着眾多自然或人為的潛在損壞因素，通常稱之為**威脅**。例如：

■ 自然威脅

災難（如火災及水災）及環境威脅（如極端的溫度及濕度）。

■ 人為威脅

人為威脅分為兩種：

有意

駭客入侵（如未經授權接達網絡資源）、欺詐（如假冒其他用戶接達網絡資源）、盜竊及惡意破壞。

無意

設備及電源故障、人為錯誤（沒有妥善保護密碼）及系統管理不善（如設備配置錯誤及軟件有漏洞）。

如果電腦系統不幸遇上威脅，可增加學校招致**損失**的風險。

現在，資訊科技設施儲存愈來愈多資料，包括儲存在學校系統的教材、學生的家課作業、重要的資訊及數據檔案等，與學校網絡融合起來。為了保護該等設施免受威脅及減低損失的風險，學校必須：

- 提高系統及網絡用戶的資訊科技保安意識，包括學生、教師、校長、學校職員，甚至學生家長，好讓他們能正確使用學校資訊科技設施；及

- 為用戶設定一套政策及程序，以保護學校的電腦系統、數據、資訊，以及硬件和軟件資產。

為協助學校實踐上述目標，本文件餘下各章旨在：

- 提供有關「**保安基礎**」的資訊；及
- 指出在學校環境中，應因應不同層次的「**資訊科技保安監控**」而採取適當程度的「**保安措施**」。

2 保安基礎

資訊科技保安可以視為「與資訊科技有關的範疇不會發生令人無法接受的風險」，這涵蓋了**技術、操作及管理**等各方面。例如說，除了系統、工作站及伺服器的正確配置及管理之外，妥善的資訊科技保安還需視乎相關政策及程序的落實遵行、實體接達控制，以及審查功能。

2.1 資訊科技保安目標

在上一章中談到，學校必須保護資訊科技設施，避免威脅，才能有效地降低損失的風險。為此，我們建議學校採納以下三個「**資訊科技保安目標**」：

- 保護敏感資訊以免那些資料在未經授權情況下披露（即**機密性**）；
- 維持數據的準確性、完整性、一致性和及時性（即**完整性**）；及
- 保護必要的資源及其相關性能（即**可用性**）。

儘管以上三個保安目標都是必須的，但學校可根據本身的情況及需求，修訂各項目標的比重。以下章節將詳盡說明這三個目標。

2.1.1 機密性

當資訊被未獲授權的人士閱讀或複製，此情況已視為機密外洩，比如說，學生未經教師授權或准許，從學校的伺服器中取得試卷的複本(電子複本)。

學校須確保用戶在獲授權情況下方可存取資訊。因此，學校的系統需要適當設定，例如，利用接達控制，甚至數據加密（即把數據轉成保密碼），以保護數據。

2.1.2 完整性

當數據意外地被修改，比如說，學校文員錯誤地更改了網上校管系統裡的一個學生編號，又或其中一個數據檔案裡的一個字符由於磁碟故障而被修改了，這些都視為數據不完整。

學校須確保數據的準確性、完整性及有效性，不能容許有未經授權修改的情況出現，無論是意外的或是惡意的。

2.1.3 可用性

資訊必須是隨時可用的，無論是為了滿足學校需求或避免重大損失的緣故。

舉例說，如果學校學與教網絡伺服器沒有配置不間斷電源供應器（UPS），在意外停電時，伺服器將不會正常關閉，亦不能正常地重新啓動，最終會導致系統不穩定或不可用，學生及教師等用戶將不能使用系統又或存取資訊。不間斷的資訊及系統資源存取是網絡系統的基本要求之一，學校須確保校內的系統及網絡能夠全面及正常運作。

2.2 資訊科技保安監控

至此，資訊科技保安的重要性及目標已十分明確。學校的系統及網絡在提供多種保安性能及選擇的同時，校方仍須檢討本身的保安需求，並作出恰當的保安決定及設置。

為實踐學校的資訊科技保安目標及需求，學校須因應不同層次的「**資訊科技保安監控**」而採取適當程度的「**保安措施**」。一些常見的資訊科技保安監控包括：

- 實體保安
- 接達控制
- 數據保安
- 網絡及通訊保安
- 保安審查及保安事故處理
- 用戶關注及教育

以下章節將概括描述上述保安監控事項。各項資訊科技保安監控的保安措施，將在本文文件往後章節詳述。

2.2.1 實體保安

實體保安是保安防禦的第一防線，防止直接存取資訊及／或入侵者避過資訊科技保安系統。

學校的資訊科技設備，如同伺服器、工作站、備份帶、復原磁碟、軟件連包裝套等，應放置在安全地方以防有人未經授權下使用。此外，學校須根據不同的實體保安需求，將校園劃分為多個不同層次的保安區域。

2.2.2 接達控制

為不同系統的不同用戶，在使用相關資源時設定不同的權限。接達控制是為特定的數據檔案、資源及其他系統權限界定及賦予使用權利。適當的接達控制可防止有人未經授權下接達系統及／或使用網絡資源。

2.2.3 數據保安

數據是學校系統及網絡的重要資產。因此，因應不同程度的保安要求，學校需要將數據分成不同級別，並採取相應措施去保護學校系統，以免遺失數據。造成數據遺失的部分潛在原因有：

- 破壞性電腦病毒
- 硬磁碟副系統故障
- 電源故障
- 軟件故障
- 意外地或惡意地使用刪除或修改指令
- 自然災害

2.2.4 網絡和通訊保安

學校內有很多系統及局部區域網絡，比如說，網上校管系統、學校學與教網絡及／或多媒體學習中心。對於這些設施，學校可能有不同的保安需求。由於各項設施有需要連結起來，學校應該審慎管理這些局部區域網絡之間的通訊。

除了校內局部區域網絡之間的保安外，學校亦須仔細地計劃與其他網絡的通訊，像遙距接達及互聯網接達等，以防範可能出現的外來入侵者。此外，學校應該妥善管理及監察用戶接達上述外部網絡或服務的情況。

2.2.5 保安審查和事故處理

保安日誌可以用來追蹤及偵測威脅的發生。定期監測及檢討學校系統及網絡，有助對資訊科技保安事故及早作出警惕。

此外，學校縱使設有適當的保安監控措施，亦不能完全避免威脅的發生；因此，學校須為保安事故作好充分準備，確保所有用戶在遇上可疑問題時，懂得向誰求助。

2.2.6 用戶關注及教育

學校資訊科技保安能否成功推行，用戶教育至為重要。倘若未能提高用戶的關注，所有的預防措施也會形同虛設。

透過設計周密及穩妥的保安教育計劃，用戶便能更有準備，第一時間避免問題的發生。

2.2.7 其他保安問題

除上述的保安監控外，學校可能還有本身獨有的保安問題。在規劃資訊科技保安時，學校需要一一考慮這些問題。

其中的例子便是**系統及應用程式保安**。學校可能安裝了不同種類的桌面及網絡操作系統（如微軟NT/視窗2000/視窗XP、蘋果 iMac、Linux等），以及度身訂造的應用程式。此等系統通常會提供簡便配置的保安程式，但另一方面，這些系統之間的配搭及合作，亦需要留意。

因此，學校的系統管理員須仔細地管理上述所有系統及應用程式，確保與學校採用的保安監控及措施相容。

2.3 權衡利弊

在詳細探討各項保安監控之前，我們需要強調，沒有任何資訊科技系統或網絡是永久安全的。我們所以採用保安措施，只是希望遇上威脅時能夠降低損失風險。

儘管沒有任何資訊科技系統是百分百安全的，但是，學校應該注意，小規模保安監控的系統，跟已有各種保安措施的系統相比，總是較為容易被入侵。因此，學校必須在有限的資源及足夠的保安之間取得平衡。

2.4 更多資訊

學校可參考以下文件，以獲取更多有關資訊科技保安的資訊：

文件名稱及連結	資料來源
與兒童上網安全相關的網址（只有中文版） http://www.edb.gov.hk/FileManager/TC/Content_2342/4a.htm	香港特別行政區政府教育統籌局（教統局）
■ Windows 2000 Technical Guidelines for School	香港特別行政區政府

<p>Network Implementation (只有英文版)</p> <p>http://resources.edb.gov.hk/iteducation/updatedoc/ITEd/w2ktechnicalguidelines.PDF</p>	教統局
<p>■ 資訊科技保安指引 (政府資訊科技總監辦公室資訊科技保安政策及指引文件編號G3)</p> <p>http://www.ogcio.gov.hk/chi/prodev/download/g3.pdf</p>	香港特別行政區政府 政府資訊科技總監辦公室
<p>■ 互聯網通訊閘保安指引 (政府資訊科技總監辦公室資訊科技保安政策及指引文件編號G50)</p> <p>http://www.ogcio.gov.hk/chi/prodev/download/g50.pdf</p>	香港特別行政區政府 政府資訊科技總監辦公室
<p>■ Legal Aspects of Computer Crimes and Information Systems Security in Hong Kong (只有英文版)</p> <p>http://www.is.cityu.edu.hk/Research/WorkingPapers/paper/9404.pdf</p>	香港城市大學

3 實體保安

實體保安是指場地的保護，以及場地內的資訊科技設備及資產的保護。它是保安的第一防線，透過將硬件、軟件及資訊保存在安全的區域內，從而防止有人未經授權下使用及接達這些設施或資訊。

實體保安是一切保安監控的最基本項目。學校中的不同區域，都有不同層次的實體保安需求，故此，學校須為校內的不同區域界定不同的進入許可權（即**安全區劃分**）。

此外，硬件、軟件及數據儲存媒體，如同伺服器、工作站、備份帶、復原磁碟、軟件連包裝套等，應存放於安全的地方，以防有人未經授權下使用。

3.1 安全區劃分

為增強保安及便於管理，學校須為校內的不同區域設定不同的進入許可權。一般來說，學校可設定三個區域：

- **公共區**

開放予所有用戶使用，比如說，放置公用電腦資訊站的走廊。

- **防護區**

開放予特定的用戶使用，例如只是教師及學校職員才可使用教員室，學生只在教師陪同下才可使用電腦室。

- **限制區**

僅開放予已獲授權的人士使用，例如同伺服器室只供系統管理員使用。

不論學校劃分了多少個安全區，每個區域都必須採取適當的保安措施。例如，在圖書館及電腦室等防護區內，必須駐有負責人如圖書館管理員及教師等，以監察資訊科技設施的使用情況。

例子

甲校伺服器室內存放了伺服器及網絡配換器等主要資訊科技設備，故甲校的系統管理員將伺服器室劃為限制區，僅獲授權的人士方可進出。系統管理員更會在無人在伺服器室時鎖上門窗。

此外，訪客或服務承辦商工程師等其他人士，須在系統管理員的陪同下，方可進入限制區，而這等進出紀錄須正確地記錄於日誌中。

3.2 硬件及軟件資產保護

限制重要系統元件的使用人數，對學校保安至為重要。以下是一些保護學校硬件及軟件資產的保安措施例子。

3.2.1 進出媒體

所有進出媒體如鑰匙及匙卡等，必須只由已獲授權人士保管並存放於安全的地方。

3.2.2 伺服器室保安

由於伺服器室的設備，包括伺服器、網絡裝置及其他的主要資訊科技設備，一般都不分晝夜地運作，所以，伺服器室應配以專用電源及後備式不間斷電源供應器。

此外，伺服器室內的空調裝置須全日24小時運作，以保持最佳的溫度及濕度。

還有，學校亦須考慮安裝其他的保安措施，如熱力及煙霧探測器、移動感應器、警報系統及滅火設備，以進一步增強保安。學校應定期檢查此等設備，以確保它們運作正常。

3.2.3 樓層設備櫃的保安

網絡裝置如配換器及集線器，應存放於可上鎖的容器內，如樓層設備櫃中，以防盜竊及有人未經授權下使用。

3.2.4 電源受損防護

學校可考慮使用電源穩壓器以保護硬件設備，包括伺服器、工作站、打印機及掃描器。

3.2.5 流動裝置

流動電腦設備如筆記簿型電腦及投映機，在缺乏適當保安措施的情況下，不應放置於無人看管的地方。舉例說，筆記簿型電腦在無人使用時，應放置於可上鎖的櫃中(如伺服器室內的筆記簿型電腦櫃及／或教員室內有關教師的辦公桌抽屜中)。

另一方面，在流動裝置使用期間，應由相關的負責人看管。

3.2.6 儲存媒體

學校應妥善保管各種儲存媒體，如備份帶、軟磁碟及唯讀光碟。儲存了敏感數據的媒體應存放於上鎖的安全地方。

3.2.7 軟件備份及備份帶

軟件程式及數據檔案的正本及備份本必須妥善保存。學校應考慮將備份本與正本分開存放，並與正本保持安全距離。此舉可減低學校在發生災難性事件時失去所有版本的可能性。

3.2.8 保安標記及設備清單

保安標記及設備清單是防止實物損失的重要措施。學校應該在所有主要硬件，如系統組件、顯示器、筆記簿型電腦、打印機、掃描器、投映機、抽取式儲存裝置等塗上明確的保安標記。

另一方面，學校應採用日誌以記錄及備存一份資訊科技設備清單，並定期盤點清單項目，包括系統配置、軟件媒體及使用許可證、網絡裝置、數據備份帶等。日誌上亦應載有設備的存放位置及狀況，如「使用中」、「借出」、「維修」、「棄置」等。倘發現有缺欠及／或出現差距，學校應立即展開調查。

在建立軟件設備清單時，學校可考慮使用軟件資產管理（SAM）工具以便蒐集資料。

3.3 更多資訊

如想獲取更多有關實體保安的資訊，請參閱：

文件名稱及連結	資料來源
<ul style="list-style-type: none">■ 資訊科技保安指引 (政府資訊科技總監辦公室資訊科技保安政策及指引文件編號G3) http://www.ogcio.gov.hk/chi/prodev/download/g3.pdf	香港特別行政區政府 政府資訊科技總監辦公室
<ul style="list-style-type: none">■ 互聯網通訊閘保安指引 (政府資訊科技總監辦公室資訊科技保安政策及指引文件編號G50) http://www.ogcio.gov.hk/chi/prodev/download/g50.pdf	香港特別行政區政府 政府資訊科技總監辦公室

4 接達控制

不同用戶在使用網絡資源時，會被授予不同的權限。接達控制是一些措施，用以界定及授權用戶接達特定的數據檔案、網絡資源如打印機、以及其他系統的使用權限如登入時間。

適當的接達控制可防止有人在未經授權下接達系統及網絡資源。在監控接達方面，一般會採取認證及授權的方式：

■ 認證

認證（有時會簡單稱為「用戶登入」）是識別用戶的過程，通常根據用戶名稱及密碼進行認證。

■ 授權

授權是授予用戶接達系統及網絡資源權限的過程，授權後，用戶便可使用網絡資源例如打印機，以及學校伺服器內的數據檔案。學校對密碼保護及接達權限的設定應加倍小心，以防有人在未經授權下接達系統及資源。

用戶必須擁有自己的身分或「**賬戶**」，以接達學校系統及網絡的資源。根據用戶在校內的角色，不同用戶可享有不同的接達權限。故此，學校應根據不同組別的用戶及電腦，設定不同的規則。

以下章節將提供更多有關賬戶管理及賬戶保安選項的資訊。

4.1 賬戶管理

學校系統及網絡有各類的用戶，包括學生、教師、校長、學校職員及系統管理員。部分學校可能還包括校外的服務承辦商及學生家長。這些用戶通常會擁有與其職能、所需服務或崗位級別相應的賬戶。

例子

教師在存取電腦資訊方面的權限應該與學生不同。另一方面，學校網絡如學校學與教網絡的管理員應擁有超越一般用戶的特殊權限，以便進行系統及網絡管理的工作。

為方便管理用戶及設定保安措施，學校須識別用戶之間的相似性，並為各用戶組別設定相關的功能。賬戶一般分為兩大類別：「**普通**」及「**特殊**」賬戶。

4.1.1 普通賬戶

每個用戶可以其個人的身份或賬戶接達學校系統及／或網絡。賬戶最基本包括了用戶名稱及密碼。

一般來說，學校賬戶分為兩類，即**網絡**及**本機賬戶**。網絡賬戶用於登入網絡，以存取網絡範圍的資源，而本機賬戶則只用於登入個別的獨立電腦，以及接達與該電腦相關的資源。

例子

甲學校使用微軟視窗 2000系統支援其學校學與教網絡。視窗 2000的網域帳戶（即網絡帳戶）是供用戶存取網絡範圍的資源，而視窗 2000的本機帳戶是供用以使用獨立電腦的資源。

除不同類別的賬戶外，賬戶亦可分為「個人」賬戶或「共享」賬戶。

■ 個人賬戶

每個擁有個人賬戶的用戶在系統中都有獨特的身分，讓他們可以靈活地循個人喜好進行用戶及數據設定。

此外，由於每個用戶都擁有一個獨特的身分，因此學校可為他們制定個別系統資源的權限；而且，用戶在系統內的活動便可被「**追蹤**」及問責。

優點

- 可為個別人士制定保安設定
- 可根據賬戶活動追蹤到有關用戶

缺點

- 大量的個人賬戶可增加賬戶管理人員的工作量

■ 共享賬戶

一組共享賬戶的用戶將會以同一身分接達系統。例如，各個上電腦課的學生可共用一個共享賬戶，如此，專為這個共享賬戶而制定的所有用戶及數據設定以及安全性權限，都適用於所有學生。

但請注意，以共享賬戶進行的活動將難以被追蹤。倘學校必須使用共享賬戶，該些賬戶須被授予**最少權限**，足夠讓賬戶持有人能執行工作便可。

優點

- 使用共享賬戶可簡化用戶管理的工作

缺點

- 難以為個別人士度身制定保安設定
- 難以根據用戶活動追蹤到用戶本人

例子

甲學校在走廊設有公用電腦資訊站，為方便操作，甲校為這些公用電腦資訊站設立一個單一共享賬戶作為登入。由於眾多用戶共用這些電腦資訊站，甲校難以追蹤這個共享賬戶的活動，故此，甲校決定賦予該共享賬戶最低的使用權限。

4.1.2 特殊賬戶

另一類別的賬戶是功能賬戶，或稱為「特殊賬戶」。特殊賬戶是為支援若干特定功能而設立的，有別於供個別人士日常使用的一般賬戶。

例子

設定賬戶－管理員賬戶及超級賬戶

在微軟視窗 2000或 NT 4.0系統中，例如預設的「管理員」賬戶以及在「管理員」和「超級賬戶」組別內的賬戶，均屬於特殊賬戶。由於該等賬戶已被預設了各種特權，故此，學校必須嚴格管理該等賬戶。

設定賬戶－訪客賬戶

在微軟視窗 2000或 NT 4.0中，一些特殊賬戶如預設的「訪客」賬戶及「訪客」組別，需要在保安上有特別的設定。有些時候，學校可根據個別的需要及更佳的保安監控，關閉該等訪客賬戶。

擔任系統管理員的教師

學校部分教師會擔任系統管理員，他們須獲分配兩個用途不同的賬戶：一個為教學而設的個人賬戶，以及一個為系統管理而設並具有管理特權的特殊賬戶。

為了更佳的保安監控，有關教師應在不同情況下使用不同的賬戶。例如，在履行教學職責，如準備教材或非為管理目的而瀏覽互聯網時，他們應使用沒有特權的個人賬戶。

另一方面，為了測試及／或排解疑難的緣故，學校一般會變更改用戶的保安選項，以測試某項功能或解決某個問題。學校必須因應個別情況，為保安設定出現偏差的賬戶作出檢討。

例子

校外／臨時賬戶

甲校需要一個校外的服務承辦商協助安裝及配置學校的學與教網絡新系統。學校學與教網絡的系統管理員為服務承辦商的工程師設立一個具高級權限的臨時賬戶，並在設立後即時關閉。

每當工程師到校工作時，系統管理員便會啟動工程師的賬戶，好讓工程師在其監督下進行系統安裝及配置工作。每次工程師妥當地完成工作及離校後，系統管理員會立即再次關閉工程師的賬戶，以防有人未經授權登入及接達網絡。

當工程師完成所有工作及甲校認為有關服務告一段落後，系統管理員便將該臨時賬戶從學校學與教網絡中刪除。

4.2 用戶保安選項

學校必須妥善處理每個賬戶，為他們分配密碼及接達權限。根據學校的需要，部分賬戶可能需要更多系統或應用上的特別保安設定。

4.2.1 密碼處理

學校須讓用戶了解，他們需要對其賬戶內進行的活動承擔責任。用戶必須保密他的密碼，否則，可能會有人利用其賬戶，以他們的名義接達甚至破壞學校系統及網絡的數據或文件。

以下列舉一些處理密碼的較佳做法：

例子

保密密碼

學校須提醒用戶，千萬別向他人洩漏密碼及把密碼寫下。另一方面，無論密碼是貯存在網絡中或透過網絡傳送時，系統管理員也須確保密碼獲妥善保護或加密。

使用複雜難猜的密碼（即安全密碼）

用戶不應選擇字典內的字詞作為密碼。此外，用戶亦嚴禁使用個人身分資料如用戶姓名作為密碼。學校應建議用戶選擇由一定數量字符組成的密碼，比如說，由字母、數字及特殊符號等八個字符組合而成的密碼。

慎防使用預設密碼

用戶在首次登入時，必須更改為其預設的密碼。此外，系統管理員必須更改软件的預設密碼，例如為微軟視窗 2000 / NT 4.0 開立的管理員賬戶，其預設密碼為「Administrator」。

設定密碼有效期

系統管理員應考慮為網絡系統的所有賬戶設定密碼有效期，以迫使用戶定期更改，例如每60天便要求用戶更改其密碼。

限制登入失敗次數

系統管理員應限制所有賬戶的登入失敗次數，以防止入侵者猜測密碼，例如，經過連續五次登入失敗後，有關的賬戶將被鎖定，以防有人繼續猜測密碼。

保護BIOS密碼

除了電腦系統或網絡的登入密碼外，每台電腦本身應設有一個BIOS及開機密碼，為硬件提供第一層保護。

系統管理員可要求承辦商預設及啟動所有電腦的 BIOS 密碼。只可向學校已獲授權的人士披露密碼的詳情。

此外，系統管理員可考慮要求用戶在使用該台電腦時，輸入 BIOS 開機密碼。

4.2.2 用戶及使用權限設定

學校須確保用戶權限，只按他們有「實際需要」這準則而設定。學校須避免為用戶開放不必要的權限，即是用戶只獲授權使用那些他們在工作上所需的資源。

下面列舉一些用戶及使用權限設定的最佳做法：

例子

設定適當權限

系統管理員應妥善管理其系統，並為用戶設定適當的權限，以使用系統及網絡資源。例如，學生不能使用教師的主目錄或使用學校辦公室內的打印機列印文件。

檢視用戶權限

用戶權限應定期檢討，系統管理員應盡快剔除不必要的權限，及盡快刪除已廢棄的賬戶。

限制登入時間

用戶只可以在有需要時，才能夠登入學校系統及網絡。例如，學校可考慮在一般的上課日子，將大部分用戶的登入時間設定為早上七時至晚上七時。

要求為所有電腦認證

除實體保安外，學校的所有系統，包括伺服器、聯網及／或獨立的工作站，以及筆記簿型電腦，都需要鍵入用戶名稱及密碼，方可接達系統。此外，用戶在非使用系統時必須登出系統及清除在登入對話框中的用戶名稱。

啓用熒幕保護

系統管理員應考慮為所有電腦強制啓用有保護密碼的熒幕保護程式。目的在預設的時間內，例如十分鐘，電腦沒有進行任何活動，便會自動上鎖，。

4.3 更多資訊

如想獲取更多有關接達控制的資訊，請參閱：

文件名稱及連結	資料來源
<ul style="list-style-type: none"> ■ 資訊科技保安指引 (政府資訊科技總監辦公室資訊科技保安政策及指引文件編號G3) http://www.ogcio.gov.hk/chi/prodev/download/g3.pdf 	香港特別行政區政府 政府資訊科技總監辦公室
<ul style="list-style-type: none"> ■ 互聯網通訊開保安指引 (政府資訊科技總監辦公室資訊科技保安政策及指引文件編號G50) http://www.ogcio.gov.hk/chi/prodev/download/g50.pdf 	香港特別行政區政府 政府資訊科技總監辦公室

5 數據保安

學校系統及網絡內的數據可能是最重的資產。在設定實體保安措施及用戶存取架構時，學校亦應關注數據保護的問題。

一般來說，數據保安需要把數據檔案妥善地建立、加上標籤、儲存及備份，同時亦要提防電腦病毒的攻擊。

以下章節旨在為學校提供一些防止遺失數據的例子。

5.1 資料分類

學校系統及網絡中的資料應根據其敏感程度分類，並為不同類別的資料設定合適的存取權限，然後根據不同用戶的需要分配存取權。

資料一般可被劃分為三個基本類別：

- **公開資料**
公開資料可供所有用戶使用，例如學校公告。
- **私人資料**
私人資料僅供資料擁有人使用，例如存放在用戶主目錄的資料檔案。
- **限制資料**
限制資料僅供預定的組別或人士使用，例如考試卷。

例子

甲校決定將儲存於伺服器中的資料分為三類，例如：

- 「公開」資料，如校曆、校巴時間表、活動安排等，所有用戶僅擁有瀏覽權；
- 「私人」資料，如各用戶主目錄儲存的檔案或文件，僅可由擁有人修改；及
- 「限制」資料，如已加密的考試卷，並僅准許有關的學科教師存取。

不過，要注意上述的資料分類僅供參考，並非適用於所有學校環境。學校可因應需要界定較多或較少的資料類別，例如有些學校認為員工考績報告需要更嚴格的數據保安要求，便將資料儲存於軟磁碟，並鎖放在安全地方。

無論在學校環境中界定了多少個資料類別，學校都必須如以下章節所描述般，妥善保護資料，以免有人未經授權嘗試存取或處理資料。

5.2 資料處理

數據保安可保護學校的系統及網絡避免遺失資料。導致資料遺失的成因可能是電腦病毒、電源或磁碟副系統或軟件故障、意外或惡意使用刪除或修改指令、天災等。

電腦病毒入侵會損害甚至銷毀資料。學校必須安裝及設定防毒軟件以保護資料免受電腦病毒入侵。本章較後部分將提及有關電腦病毒防護的詳細資料。

另一方面，因儲存媒體的損壞或電源故障而造成的資料遺失及網絡斷線，可分別透過設置高階的硬磁碟副系統及不間斷電源供應器等保安措施以加強防護。至於遇到資料遺失或遭受破壞時，也可利用備份及進行復原程序修復有關資料。

5.2.1 儲存於伺服器的資料

學校網絡的伺服器被視為系統的核心所在。伺服器中那些對所有網絡用戶至關重要的資料，尤其需要妥善保護，因此，學校應考慮使用先進的技術以減少磁碟錯誤，(例如使用冗餘磁碟陣 (RAID) 硬磁碟副系統)，及保持服務 (如不間斷電源供應器)。

5.2.2 資料備份及復原

學校須制定妥善的「系統備份及復原」策略，使已受破壞或遭意外刪除的資料可從相應的備份中復原。

該策略應訂明備份及復原所有重要資料的步驟與程序。有關程序應可全自動進行及盡少涉及人手操作。此外，所有備份及復原程序均應記錄在案、通過檢測並妥善執行。

學校須**指派專人** (如技術支援服務人員或系統管理員) **負責資料備份及復原**。有關人員應定期備份及監測資料，亦宜定期進行復原測試，以確保備份檔案可以復原資料。

此外，如在「實體保安」一章所述，學校必須將備份媒體 (如備份帶) 貯存於安全地方，例如，每次進行資料備份 (通常在午夜自動執行) 後，技術支援服務人員應盡快 (通常為翌日早上) 從備份裝置中取出備份媒體，然後交予負責教職員或系統管理員，或甚至校長，以貯存於可上鎖的櫃中，而非讓備份媒體留在伺服器室內。。

學校亦可考慮把備份媒體貯存於「校外地方」，即與正本保持一定安全距離的地方，這做法可減低因學校發生災難性事故而引致失去所有備份的機會。

有關資料備份及復原的詳細資料可參考「學校區域網絡實施技術指引—視窗2000版」(只有英文版)，而磁帶輪換計劃可參考以下連結：

<http://resources.edb.gov.hk/iteducation/updatedoc/ITEd/w2ktechnicalguidelines.PDF>

5.2.3 儲存媒體的標籤及貯存

學校須根據不同的資料類別，為儲存媒體如備份帶、軟磁碟及唯讀光碟等加貼標籤，並按以上章節所述，因應資料的類別，妥善存放有關的儲存媒體。

5.2.4 敏感資料的保護及棄置

學校可考慮透過檔案加密 (如微軟視窗2000的資料加密功能：加密檔案系統(EFS)) 以提高敏感資料的保安級別。

此外，學校可考慮使用在某些應用軟件 (如微軟辦公室套件的程式) 的密碼保護功能，以保護含有敏感資料的文件。

另外，在棄置或銷毀儲存媒體之前，學校必須徹底清除所有敏感資料。

5.2.5 保護個人資料的原則

《個人資料（私隱）條例》適用於資料使用者，即任何蒐集、持有、處理及使用公營及私營機構，包括政府部門的個人資料的人士。根據條例規定，資料使用者必須遵守六項符合國際慣例的保障資料原則來處理及使用個人資料。該些原則詳見於以下網址：
http://www.pcpd.org.hk/chinese/ordinance/section_76.html.

其中第4項原則是有關個人資料的保安，訂明資料使用者須採取適當的保安措施來保障個人資料。根據該項原則，學校須防止有人未經授權擅自或意外地查閱、刪除、處理或以其他方式使用學校持有的個人資料。學校亦須考慮保護

- 所持有的[個人資料](#)；
- 所處理的[資料](#)；及
- 所傳送的[資料](#)。

與《個人資料（私隱）條例》有關的資訊	資料來源
http://www.pcpd.org.hk/ .	香港個人資料私隱專員公署
http://www.privacy.com.hk/	Privacy of Personal Data in Hong Kong
https://www.pcpd.org.hk/chinese/ordinance/down.html	個人資料（私隱）條例
http://www.dutylawyer.org.hk/ch/tellaw/law7.asp?id=75&ver=ch&category=general	香港特別行政區當值律師服務的《個人資料（私隱）條例》資訊

5.3 預防電腦病毒

電腦病毒是一些電腦程式，專為破壞其他電腦程式或資訊，或因惡作劇而編寫。這些程式如同真實病毒一樣，可自行複製並散播到其他的電腦。它可透過破壞甚至銷毀學校系統及網絡數據而影響其正常運作。

電腦病毒按其駐留、散播方式及對電腦造成的損害，分為很多不同種類，例如，開機磁區病毒會先駐留在儲存器的開機磁區，之後載入電腦記憶體進行感染。

以下是一些保護資料免受電腦病毒入侵的較佳方法。

5.3.1 防毒軟件

所有學校電腦系統，包括伺服器及客戶工作站（桌上電腦及筆記簿型電腦）均應安裝常駐記憶體的防毒軟件，並應啟動病毒監測及實時預警功能，這樣可使學校系統在載入及使用軟件及資料檔案前，進行防毒掃描。

學校亦須定期更新防毒軟件的病毒定義檔。有關詳情將在本章較後部分討論。

5.3.2 合法及經授權使用的軟件和硬件

學校電腦及學校網絡應只運行來自可靠來源及或獲授權代理的軟件。盜版軟件是主要的病毒來源，學校必須禁止使用盜版軟件。

除盜版軟件外，學校亦應當避免使用未經授權的軟件及硬件。未經校方的預先批准，不得在校內使用個人授權軟件，或是個人電腦（如教師的個人筆記簿型電腦）。

此外，學校須確保該等個人軟件及硬件在安裝或連接至學校系統及網絡之前，均獲授權使用以及並沒有感染病毒。

5.3.3 遠離可疑檔案資源

如今透過電子郵件（電郵）通訊已是十分普遍。學生及教師可使用網絡瀏覽器（如利用微軟Internet Explorer及Netscape Navigator閱讀網上電郵）及／或閱讀電郵軟件（如Microsoft Outlook）隨意在互聯網上與任何人「交談」，也可透過電郵交換資料檔案，即電郵附件。

此外，用戶亦可能使用校內的電腦系統接達萬維網（WWW），下載程式軟件試用（如來自互聯網的免費軟件或共享軟件）。

學校須注意電郵附件或是互聯網上的軟件程式，尤其是不明來源，副檔名為「.exe」、「.com」及「.vbs」的檔案，都是最常見包含病毒的來源。這些文件及軟件程式在使用前必先要經過病毒檢查並將所發現的病毒清除。

此外，在使用不明來源的如軟磁碟及唯讀光碟資料檔案前，亦須經過病毒掃描並將所發現的病毒清除。

5.3.4 用戶教育及事故處理

用戶不得故意編寫、製作、複製、散播、執行或引入電腦病毒。但用戶很可能透過下載檔案及／或開啓互聯網電郵，或在學校電腦開啓從家中的個人電腦複製的檔案，因而誤將病毒引入學校系統。因此，保護學校系統遠離病毒的最佳方法之一，便是教育用戶。

學校應教授用戶有關病毒的知識，讓他們認識到病毒可做成的損害，並應要求用戶在發現病毒後立即報告。此外，若懷疑電腦受病毒感染，應停止使用該電腦及／或中斷其網絡的連線，並設法盡快清除電腦病毒。

有關處理病毒感染的更多資訊，將於「保安審查及保安事故處理」一章討論。

5.4 軟件配置及更改監控

學校應對系統及網絡實施**積極主動的保安措施**，例如：

5.4.1 關閉或刪除所有不必要的服務及組件

「完全」或「典型」安裝微軟視窗XP、2000或NT伺服器或專業版或工作站版時，以及安裝一些應用程式如微軟 FrontPage，可能會自動啓動了微軟Internet Information Service Server（IIS）及其他與互聯網相關服務的安裝，如FTP、SMTP、NNTP、網上列印、索引服務等。

在很多情況下，學校實際上不需要這些服務或組件。然而，疏忽設定該等服務或組件經常會導致保安漏洞。因此建議學校關閉或移除這些對學校系統沒有功用及不必要的服務或組件。

5.4.2 使用管理工具

一些微軟視窗XP、2000或NT 4.0的內置功能及管理工具，如「漫遊設定檔」、「網域用戶管理」、「系統策略編輯器」、群組原則等，都對保安配置及桌面管理有幫助。系統管理員可使用這些工具度身制定賬戶及設定（即用戶設定檔），並限制用戶更改任何的系統設定。

例如，系統管理員可使用這些工具統一所有用戶或各組用戶的用戶介面（如「開始」選單、桌面圖示、壁紙、螢幕保護等）。

此外，這些工具亦有助系統管理員限制用戶更改任何桌面設定、系統檔案及應用程式。例如，系統管理員可移除「接達控制台」裡「顯示」及「系統」的項目，以防學生更改電腦的系統配置及網絡設定。

5.4.3 應用備受推薦的保安漏洞修正方案

學校要注意，沒有軟件是「永久可靠」的。學校應留意有關資訊科技保安方面的最新資訊，如有備受推薦的保安漏洞修正方案，應該在學校系統中應用。

5.4.3.1 病毒定義檔

學校需定期瀏覽防毒軟件網站，並檢查有否病毒預警或最新的病毒定義檔，並且應定期更新所有電腦的病毒定義檔，例如，**至少每週一次**。

下列網站是提供最新病毒資訊及預警的機構及防毒軟件公司：

病毒預警	資料來源
http://www.hkcert.org/valert/valert1.html	香港電腦保安事故協調中心
http://www.cert.org/current/current_activity.html#virus	The Computer Emergency Response Team Coordination Center
http://www.f-secure.com/virus-info/	F-Secure Corporation
http://www.mcafee.com/anti-virus/	McAfee.com Corporation
http://www.symantec.com/zh/cn/enterprise/security_response/index.jsp	Symantec Corporation
http://www.trendmicro.com/vinfo/zh-tw/	趨勢科技股份有限公司

5.4.3.2 軟件修補程式

學校需注意在學校系統及網絡內已安裝的軟件中，可能存在程式錯誤及保安漏洞，故應定期瀏覽軟件供應商及一些保安機構的網站，以取得最新的保安警報。

下列網站是提供最新保安警報的機構及軟件公司：

保安公告	資料來源
------	------

http://www.hkcert.org/salert/salert1.html	香港電腦保安事故協調中心
http://www.microsoft.com/china/technet/Security/default.mspx	微軟公司

若發布了新的保安方案或系統修補程式，學校應仔細閱讀有關的資料，並考慮在學校系統使用這些方案及安裝修補程式。

例如，**網頁瀏覽器**（如微軟Internet Explorer及Netscape Navigator）、**閱讀電郵軟件**（如微軟Outlook）、**網頁伺服器**（如微軟Information Internet Server）及**操作系統**（如微軟視窗XP、2000或NT 4.0）均是一些學校需要特別注意的常用軟件。

微軟提供一些保安檢驗程式，供評估系統保安狀況，及建議必要安裝的軟件修補程式（如有）。下列保安檢驗程式可能對檢驗學校系統有幫助。

保安檢驗的附加工具	資料來源
<ul style="list-style-type: none"> ■ 微軟基準安全分析器 這是一項網上網絡應用程式，以檢驗視窗2000及XP系統，並提供一份保安設定及改善建議的報告。 http://www.microsoft.com/china/technet/security/tools/mbsahome.mspx ■ Microsoft Network Security Hotfix Checker (Hfnetchk.exe) Tool 這是一項以指令操控的工具，學校系統管理員可用以進行中央評估，檢視安裝了視窗XP、2000或NT、Internet Information Server 4/5、Internet Explorer 5.01或更新版本等的一台電腦以至一組電腦，是否擁有或缺乏有關保安修補程式。 http://www.microsoft.com/technet/security/tools/hfnetchk.mspx 	微軟公司

5.4.3.3 訂閱保安警報電郵

要積極及安全地使用電腦，學校應訂閱由保安機構或軟件公司發出的保安警報電郵。學校應為全體有關負責人員訂閱，包括系統管理員及支援學校學與教網絡的員工。

學校亦可從防毒軟件公司（見下列網站）訂閱保安警報。

訂閱保安警報	資料來源
https://www.hkcert.org/subscribe/home.html	香港電腦保安事故協調中心

5.5 更多資訊

如想獲得更多有關數據保安的資訊，請參閱：

文件名稱及連結	資料來源
<ul style="list-style-type: none"> ■ 資訊科技保安指引 （政府資訊科技總監辦公室資訊科技保安政策及指引 文件編號G3） 	香港特別行政區政府 政府資訊科技總監辦公室

http://www.ogcio.gov.hk/chi/prodev/download/g3.pdf	
<ul style="list-style-type: none"> ■ 互聯網通訊保安指引 (政府資訊科技總監辦公室資訊科技保安政策及指引 文件編號G50) http://www.ogcio.gov.hk/chi/prodev/download/g50.pdf	香港特別行政區政府 政府資訊科技總監辦公室

此外，學校可參考下列文件，以獲取更多有關電腦防毒保護的資訊：

文件名稱及連結	資料來源
<ul style="list-style-type: none"> ■ 電腦病毒的種類 http://www.infosec.gov.hk/chinese/general/virus/type.htm 	香港特別行政區政府
<ul style="list-style-type: none"> ■ 惡作劇電子郵件 (惡作劇訊息是虛假的病毒警告，通常以電郵形式出現) http://www.infosec.gov.hk/chinese/general/virus/hoax.htm 	香港特別行政區政府
<ul style="list-style-type: none"> ■ 預防電腦病毒指引及資料 http://www.infosec.gov.hk/chinese/general/virus/guideline.htm 	香港特別行政區政府

6 網絡和通訊保安

能夠遙距接達學校的系統及網絡，以及存取互聯網內的資源，對學校是有用及有幫助的；但缺點是學校系統容易遭受外界的攻擊。

除了學校與外界網絡之連接外，校內亦有不少局部區域網絡是相互連接的，例如，學校學與教網絡、多媒體學習中心和網上校管系統。學校可因應情況，設定不同局部區域網絡的保安需求。

因此，學校應謹慎管理學校與**外界網絡**，以及學校**局部區域網絡**內不同元件之間的通訊。同時須採取適當的保安措施，以保護及監控有關的通訊。

6.1 學校與外界網絡之間的通訊

互聯網內有大量資源，大部分學校均已透過不同的方式連接這「資訊高速公路」，例如，透過傳統電話線與調制解調器、專線或寬頻連接等。

此外，有些學校容許用戶在校外**遙距接達**學校系統及網絡。例如，在某些緊急情況下，系統管理員須於夜間用家中的電腦，遙距管理學校學與教網絡。

學校應實施適當的保安措施，以防學校網絡遭受外界攻擊。此外，學校應教導用戶如何使用該些外界網絡並監察他們的接達情況。

6.1.1 遙距接達

學校主要設有兩種遙距接達，分別為：

- **撥入接達**

透過撥號設備（如電話線及連接調制解調器的電腦），即使用戶在遠處（如在家中），也可撥入連接至其學校的網絡工作，與身處校內直接連接局部區域網絡環境無異。

- **撥出接達**

透過撥號設備（如電話線及連接調制解調器的電腦），校內用戶可撥出連接至其他電腦網絡（如互聯網）。

6.1.1.1 撥入監控

學校應只限獲授權人士透過撥入接達學校網絡。學校應安裝中央撥入伺服器（如裝有遙距接達服務（RAS）的視窗 2003/2000/NT 伺服器），以支援撥入接達。

學校亦應在系統中採取適當的保安措施，例如設定回撥功能及審查日誌。學校應定期檢查審查日誌，查看有否任何企圖入侵系統的情況。

6.1.1.2 撥出監控

校內用戶不得在聯網電腦使用撥出功能。若需要撥出功能，應透過中央撥出伺服器（如視窗 2003／2000／NT RAS或接連多條電話線上網的單IP分享器）進行，並作出定期審查。倘學校沒有裝設中央撥出伺服器，則應在獨立的電腦或系統中進行撥出接達。

此外，學校應嚴密地監控撥出設備。

6.1.1.3 其他要點

學校不應將同一撥號設備同時用作撥入及撥出。撥入及撥出使用不同的撥號設備，較易監測及追蹤撥號活動。非使用中的調制解調器應關掉電源。

6.1.2 接達互聯網

學校可能已透過電話撥號、專線或寬頻，連接互聯網，以接達網上資源及／或建立學校網站。

然而，實在無法保證惡意入侵的駭客不會透過互聯網的連接來攻擊學校網絡。另外，學校亦難以查知校內用戶會使用互聯網搜尋引擎存取哪些資訊內容。

故此，不論學校使用哪種連接互聯網的方式，都應採取適當的保安措施。

學校應透過一個中央**互聯網通訊閘**把校內網絡／伺服器與互聯網連接起來，並設定足夠的保安措施，如**互聯網服務及網站過濾等**。此外，學校應定期檢查所有相關設定，以及所產生的**審查日誌**。

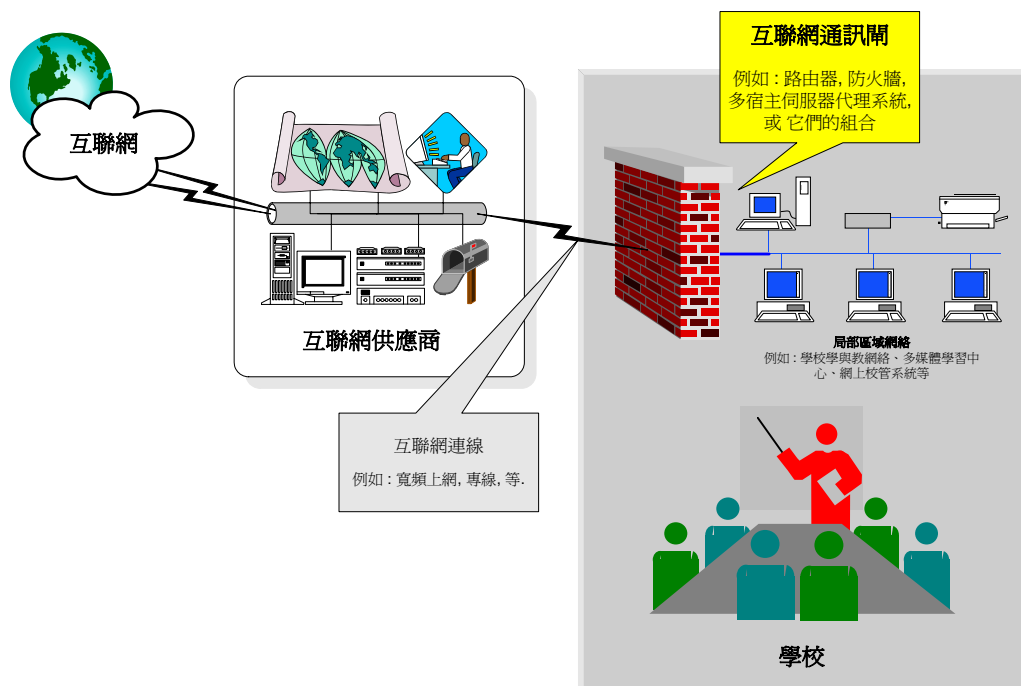
我們建議學校在籌劃／設計互聯網保安時，向服務承辦商尋求專業意見。

6.1.2.1 互聯網通訊閘

一般而言，「**互聯網通訊閘**」由硬件和軟件組成，作為私人網絡與互聯網之間的橋樑，並保護私人網絡避免入侵。

互聯網通訊閘是擔當管理員角色，根據用戶設定的保安準則（稱為「**規則集**」）控制私人網絡與互聯網之間的數據傳輸。**互聯網通訊閘**會截取並代為執行內部網絡對互聯網發出的指示，然後把資訊發回給內部網絡的用戶。倘若有外來的駭客試圖入侵私人網絡，**互聯網通訊閘**會拒絕該駭客接達的要求。

舉例說，學校的**互聯網通訊閘**擔當著學校學與教網絡（即私人網絡）與互聯網之間的中間人角色，監控兩者之間的數據傳輸；所有進出學與教網絡的數據均須通過**互聯網通訊閘**，從而檢查，並攔截那些違反規則集的數據。



互聯網通訊閘的類型

學校可透過不同方式設置互聯網通訊閘。有些學校簡單地選擇使用**路由器**作為學校互聯網通訊閘；而有些則使用**防火牆系統**、**多宿主伺服器代理系統**，或以上述設備組合，以增強保安防護。

以下簡述各種類型的互聯網通訊閘：

■ 路由器

典型的硬件路由器是簡單及價錢相宜的互聯網通訊閘。該路由器最少需要兩個介面：一個用作連接學校網絡，另一個用作連接互聯網。

事實上，互聯網服務供應商借用的路由器本身便可用作互聯網通訊閘。然而，學校或會發覺透過路由器來設定複雜的數據過濾（如規則集）是相當困難的。此外，有些互聯網服務供應商可能會在服務協議條文內訂明不准用戶更改路由器的設定。

■ 防火牆系統

防火牆系統可以在一個「黑盒」裝置內執行，或在已安裝有關軟件的電腦上執行。

防火牆技術分多種類型，例如封包過濾（如IP網絡地址）及應用程式過濾（或稱通訊協議過濾）（如「FTP」及「Telnet」）。學校可設定規則集以過濾及監控學校與互聯網之間的封包及應用程式。

例如，學校可利用防火牆及設定合適的規則集，以防止學生接達一些特定的網站（如涉及色情及暴力的網站），或關閉服務如「Telnet」及「ICQ」等，以禁止ICQ通訊及遙距接達。

■ 多宿主伺服器代理系統

多宿主伺服器代理系統通常是配有**兩張網絡介面卡**的隔離式伺服器代理系統（它可以是一部低檔次的伺服器，或是一部只有足夠資源運作的工作站），安裝並接連於學校與互聯網中間。

多宿主伺服器代理系統可根據用戶設定的規則集來過濾及監控封包及應用程式，這與防火牆系統近似。但多宿主伺服器代理系統有時只能設定有限的規則集。

附註

一般而言，代理伺服器系統是在客戶應用程式（如網頁瀏覽器）與真正伺服器（如網絡伺服器）之間的一個伺服器。例如，一個學校代理伺服器系統會截取從學生電腦內的網頁瀏覽器所發出的請求，然後系統會作為學生電腦的代表，將該項請求轉發至校外的網絡伺服器。

代理伺服器系統常用於以下兩大用途：

- **提升網絡接達表現**（網頁快取）：代理伺服器系統純粹取回先前請求／用戶已拿取（快取）的網頁／內容，而毋須向（外界的）網絡伺服器轉送有關的網絡請求。
- **過濾請求**：即本節中所述的多宿主伺服器代理系統。

精密的代理伺服器系統可同時提供以上兩種服務，例如，在資訊科技教育計劃下標準供應的代理伺服器軟件（如微軟代理伺服器及Netscape代理伺服器）。然而，學校應注意除了代理伺服器軟件之外，亦要另行安裝及設定客戶端軟件。

哪種互聯網通訊閘最為安全？

這個問題並無絕對答案，視乎學校的情況及保安需求，上述任何一項或組合以上各項，均可用作為學校的互聯網通訊閘。

下表會就路由器、防火牆及多宿主伺服器代理系統用作互聯網通訊閘，作出扼要的比較：

種類	優點	缺點	備註
路由器	成本低（互聯網服務供應商會免費借用）。	難以設定複雜的配置。	有些學校或會認為單靠路由器不足以防護互聯網。
防火牆系統	可設定擴展過濾規則集。	需專業技術。 相對昂貴。	儘管防火牆系統或要額外增加成本，有些學校仍會選擇使用以增強對互聯網的保護。 用現成可買的「黑盒」式裝置，或在電腦上安裝防火牆軟件。
多宿主伺服器代理系統	更可用作內容快取。	需專業技術。	單介面代理伺服器系統（即只有一張網絡介面卡）通常只能用作內容快取，不可作為互聯網通訊閘。 儘管許多學校使用多宿主伺服器代理系統作為保安解決方案，但其實它並不包含高端防火牆方案所提供的所有功能。 一般而言，在電腦上安裝伺服器代理軟件是必須的。然而，多宿主伺服器代理系統不應安裝在視窗 2000或NT的網域控制器（DC）上。

成本

以往單是一組高級防火牆軟件系統便要耗資數萬港元，其專用硬件的成本更是讓人卻步。但近年來，防火牆價格日益低廉及普及。許多硬件製造商及軟件開發商皆能夠生產

價廉但精密，並適用於中小型企業以至個人、家庭或學校系統的小型／家庭辦公室（SOHO）防火牆。

硬件互聯網通訊閘與軟件互聯網通訊閘

實際上，許多製造商或開發商會同時使用上述兩種或以上的技術以建立互聯網通訊閘。其中一些便是所謂的「全能組合」硬件互聯網通訊閘／共享／防火牆／代理裝置，可以用作為「黑盒」並將學校網絡／伺服器與互聯網連結起來；也有一些是以軟件為主，並需要在電腦內運作。此外，有些軟件屬免費軟件（提供有限功能），而有些則須付款（提供全部功能）。

以下的對照表扼要地說明了硬件及軟件式互聯網通訊閘的主要優點：

互聯網通訊閘	優點
<ul style="list-style-type: none"> ■ 硬件 	<p>多元化服務。供應商經常在一種裝置中包含不同的服務（如路由器、防火牆、代理、配換器／集線器、用以分配及管理IP網絡地址的動態主機配置協議伺服器(DHCP)等）。</p> <p>容易安裝。只要將裝置插入學校的局部區域網絡，然後稍作伺服器設定，該裝置便可運作。毋須附加伺服器（或高端工作站）及其周邊設備。</p> <p>易於使用。一般為軟件配置設有網絡介面，該裝置可不時透過供應商網站下載的軟件作更新。</p>
<ul style="list-style-type: none"> ■ 軟件 	<p>完全監控。軟件式互聯網通訊閘提供完全監控功能，可設定各種選項。</p> <p>監控用戶。軟件式互聯網通訊閘通常可從網絡（如視窗 2000／NT 4.0）提取賬戶及保安設定資料，能更深入地對用戶作出監控。</p> <p>較佳的審查日誌及報告。軟件式互聯網通訊閘常具備綜合的審查功能，有助系統管理員監測進出學校網絡的數據傳輸，以及提升網絡效率，並在懷疑存在保安事故時分析日誌。</p> <p>較佳的整合。有些軟件式互聯網通訊閘可與其他供應商的產品整合成單一（或多重）伺服器。這種協作方向較單一的硬件裝置方案，更能保障網絡的安全。</p>

例子

甲校的網絡以寬頻上網，而寄存在學校伺服器內的學校網站亦管有許多重要的教育資源。由於學生及教師在家中，以至很多的訪客也可經常瀏覽該網站，甲校決定安裝防火牆「黑盒」，以保護其學校系統及網絡。

防火牆輔以互聯網服務供應商借用的**路由器**，以及學校的**代理伺服器系統**，可為甲校提供一個更佳的保安及網絡接達解決方案。

6.1.2.2 過濾

如上文所述，學校應採用適當的過濾服務以進一步保障接達互聯網的安全。過濾服務有多種，如**互聯網應用程式／協議過濾**、**網站過濾**以及**網頁內容過濾**等。

無論學校計劃採用哪種過濾服務，也應確保實施以下政策—只授予用戶在執行工作時所需的接達權。

互聯網應用程式／協議過濾

防火牆及多宿主伺服器代理系統可監控及過濾互聯網服務及學校與互聯網之間的通訊協議，包括接達網絡所用的「HTTP」協議、電郵所用的「POP」及「SMTP」協議、檔案傳輸所用的「FTP」協議、遙距登入所用的「Telnet」協議，新聞討論所用的「NNTP」協議，以及即時訊息所用的「ICQ」等。

學校可限制只准許高年級學生（如小學四至六年級）從互聯網上瀏覽多媒體內容，另准許學校所有用戶接達萬維網網頁，以及禁止所有用戶使用校內工作站透過ICQ與校外人士聊天。

網站過濾

一般而言，網站過濾可在以下一種或兩種情況下進行：

■ 透過學校的防火牆／多宿主伺服器代理系統

學校的防火牆或多宿主伺服器代理系統可監察用戶使用互聯網的情況，並阻止他們接達不恰當的網站。學校透過防火牆或多宿主伺服器代理系統中配置的預設網站評級名單，過濾不恰當的網站。

■ 透過互聯網服務供應商

在香港，許多互聯網服務供應商都特別為教育界提供網站過濾服務，毋須額外收費。其中一些甚至提供每日檢討及修訂過濾名單的服務。

在獲取或評估互聯網服務供應商的互聯網服務建議時，學校應考慮採用該等服務以過濾不恰當的網站。

下表列出了上述兩種過濾服務的一些特點：

網站過濾方法	特點
<ul style="list-style-type: none"> ■ 學校的防火牆／多宿主伺服器代理系統 	<p>每所學校的過濾名單都是獨有的，學校亦可方便快捷地作出設定（包括：增補、修改及刪除）名單。</p> <p>修改及配置方面更易於處理及更具靈活性。</p> <p>修訂過濾名單會導致額外的行政管理工作量。</p> <p>系統部署及保養需一定成本。</p>
<ul style="list-style-type: none"> ■ 互聯網服務供應商 	<p>為教育界設定主要及理想過濾名單。</p> <p>學校可就過濾名單向互聯網服務供應商提供及建議相關的增補、修改或刪除。</p> <p>過濾名單的修訂視乎互聯網服務供應商的表現及管理。</p> <p>行政管理工作可完全交予互聯網服務供應商處理。</p> <p>這通常是互聯網服務供應商提供的一項免費服務。</p>

網頁內容過濾

一些網頁瀏覽器（如微軟Internet Explorer）支援評級標準，例如萬維網聯盟（W3C）認可的網絡內容選擇平台（PICS）。學校可參照該等評級標準，就網頁內容的語言、裸露、色情及暴力各方面，選取不同程度的容許標準。

學校可按此為學校電腦內的網頁瀏覽器設定合適的評級標準，以致無論用戶何時瀏覽載有不恰當內容的網站時，其接達便會受到限制。

學校應定期檢查及修訂符合學校需求的評級標準。然而，若這種「非中央」設定實行於每台電腦中，或會增添額外的行政工作。

行政及管理

為能夠便於管理，一些防火牆及多宿主伺服器代理系統會利用學校系統內的賬戶，並按照學校的計劃，設定哪些學生、教師或群組，可使用何種服務。

例如學校可從微軟視窗 XP及／或2000及／或NT 4.0教與學學校網絡中，選擇用戶或群組，並以相應的互聯網應用程式，及／或在防火牆／多宿主伺服器代理系統中的網站過濾設定，對用戶進行中央行政管理。

此外，在大多數情況下，學校亦需在學生及教師的電腦中進行軟件安裝及／或網頁瀏覽器設定（如設定代理伺服器地址）。學校可使用行政管理工具如微軟Internet Explorer管理員工具包（簡稱IEAK，僅限微軟Internet Explorer使用），以簡化設定程序及方便安裝。

6.1.2.3 日誌紀錄及審查

審查日誌對處理保安事故至為重要。學校應啓用互聯網通訊閘的審查功能，以追蹤通過此閘的服務及接達。

學校可記錄成功及／或失敗的事件，以追蹤惡意及違反保安規定的活動。時間、日期、用戶名稱、應用協議、TCP/IP埠數，以及來源地及目的地域名及IP網絡地址等資料亦全部都可以紀錄。

學校亦應定期檢查審查日誌，以加強互聯網保安。另在「保安審查和保安事故處理」一章中，將有更多相關資訊的討論。

6.1.2.4 用戶教育

互聯網上存有大量有用的資源，學校用戶很有可能接達並用作學與教的用途。然而，使用互聯網亦會引申一些問題，如學校用戶（尤其是學生）在離開課室後所接達的互聯網資源。

有關正確使用互聯網的更多資訊，將在「用戶意識及教育」一章節中討論。

6.2 學校的局部區域網絡

學校設有許多系統及局部區域網絡，例如網上校管系統、學校學與教網絡，及／或多媒體學習中心。倘若學校對各個系統均有不同的保安要求，而又需要將它們相互連接起來，學校便應謹慎管理這些局部區域網絡之間的通訊。

6.2.1 相同保安級別的局部區域網絡

管理多個具相同保安要求的局部區域網絡並非難事。例如只要一個網絡配換器或集線器便可將該些局部區域網絡簡單地連接起來。該等局部區域網絡之間的數據傳輸可透過網絡配換器或集線器直接互相傳送。

例子

背景

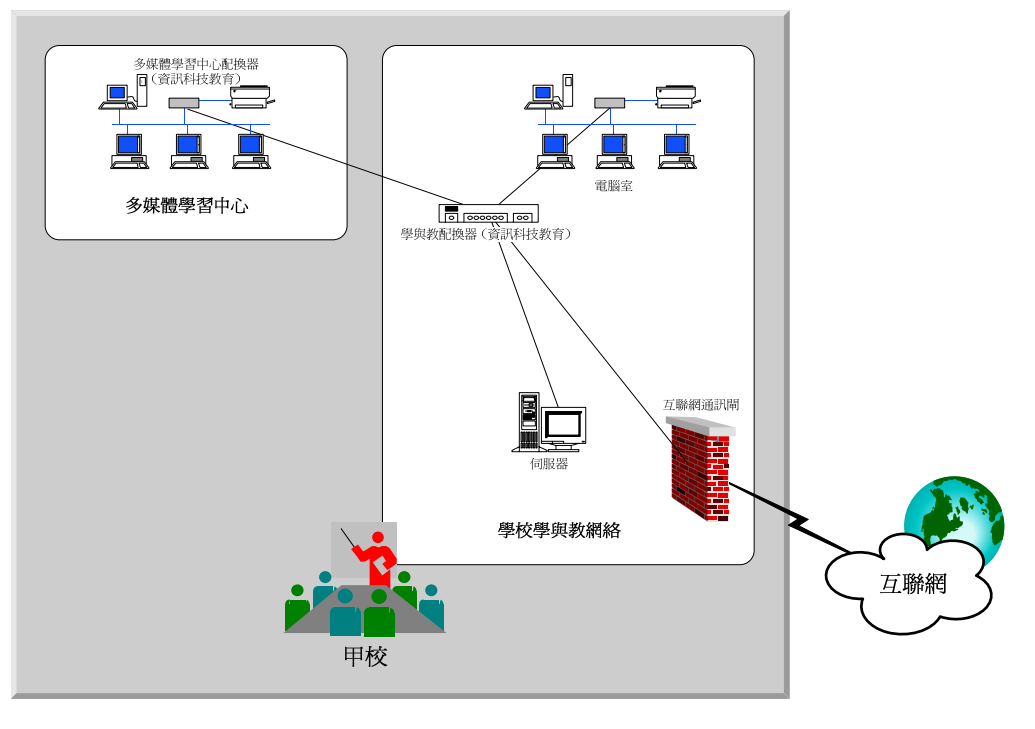
甲校設有多媒體學習中心及學校學與教網絡（工作站主要設置於電腦室內），而這兩個局部區域網絡均採用微軟視窗 2000操作。此外，學校學與教網絡與互聯網相連接。

需求

為善用資源，多媒體學習中心的用戶均需透過學校學與教網絡連接上網。

解決方案

由於這兩個局部區域網絡在甲校同屬相等的保安級別，故系統管理員決定將這兩個網絡連接至網絡骨幹配換器，以直接進行數據交換及通訊。



6.2.2 不同保安級別的局部區域網絡

然而，若各個局部區域網絡具有不同的保安要求，在把它們相互連接之先，學校**必須進行若干設定**。

例如，根據學校的情況，一些保安措施如接達監控裝置（ACD）（如路由器、路由配換器、防火牆系統，或以上各項的組合），其作用類似上文曾論述的互聯網通訊閘，可以用作監控及保護該等局部區域網絡之間的數據傳輸。

此外，對於不同保安級別的局部區域網絡之間的數據交換與通訊，尚有其他方法可以作出監控，例如為在該等局部區域網絡中使用的電腦系統配置合適的保安設定（如在微軟視窗 2000或NT網域中建立信託關係）。

在計劃連接及管理不同保安級別的局部區域網絡時，學校宜先諮詢服務承辦商的意見。

例子**背景**

除了多媒體學習中心及學校學與教網絡之外，在前一例子中的甲校另有一個局部區域網絡—網上校管系統。在微軟視窗 2000 Professional（客戶端電腦）及 NT 4.0伺服器

(伺服器)上應用的網上校管系統視窗2000版，旨在儲存及處理敏感的行政管理數據，並嚴禁未經授權接達網上校管系統。故此，網上校管系統起初是與其他局部區域網絡隔離的。

需求

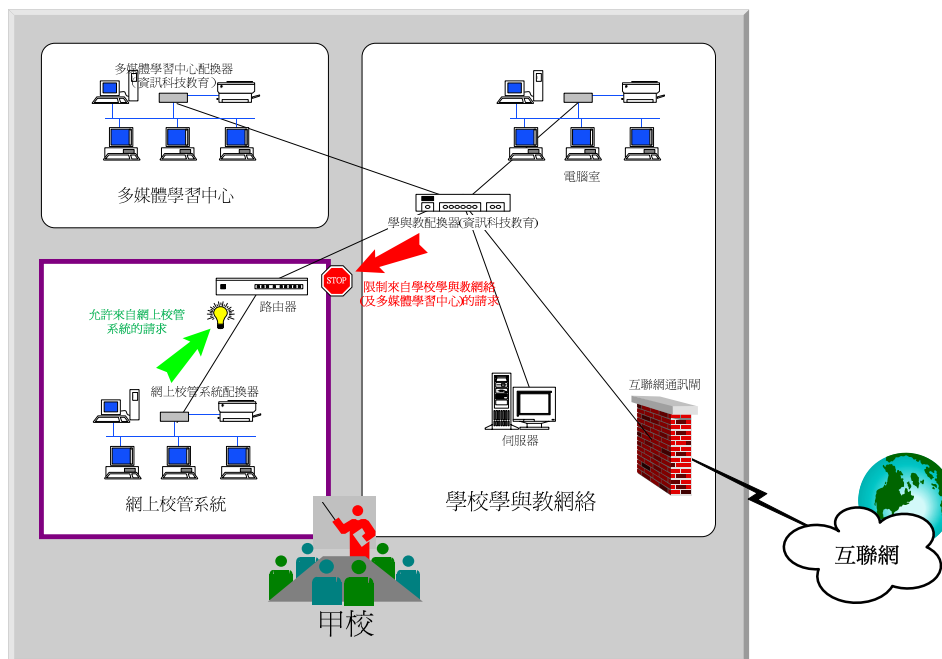
為更好地分享及善用資源，網上校管系統的用戶需透過互聯網接達萬維網網頁，以及學校學與教網絡中的數據檔案。因此，甲校有需要將網上校管系統和學校學與教網絡相互連接於一起。

然而，由於該等局部區域網絡各屬不同的保安級別，故網絡之間須裝有接達監控裝置，以監控有關數據交換及通訊。

接達監控裝置須符合甲校的要求，一方面允許用戶從網上校管系統向學校學與教網絡發出請求（如接達萬維網網頁及檔案存取），但同時須禁止從學校學與教網絡（以及其他相同保安級別的已接連局部區域網絡）向網上校管系統發出請求。

解決方案

學校可採取不同的保安措施作為接達監控裝置。在諮詢過服務承辦商、分析過有關網上校管系統及資訊科技教育網絡整合文件（見下文附註）、並考慮過學校的特殊情況後，系統管理員決定使用路由器作為接達監控裝置。



除了一些需要預先配置工作之外，指定承辦商為路由器設定合適的規則集，並為在該等局部區域網絡中使用的系統實施適當的保安設定（如本例子中的微軟視窗 2000及NT中的信託關係建立及接達監控設定）。

經過多次測試，甲校發現以上方案可完全滿足學校的需求。隨後，系統管理員向用戶提供相關操作程序的培訓。現在，網上校管系統用戶可從學校學與教網絡中接連上網，以存取檔案及接達萬維網網頁，而同時學校學與教網絡（及多媒體學習中心）的用戶則不能接達網上校管系統。

附註

本例僅從高層次描述了為連接網上校管系統與資訊科技教育網絡而採取的保安措施及安排。有關網上校管系統的更多資訊，請參閱教育統籌局網上校管系統網址：

<http://www.edb.gov.hk/index.aspx?nodeID=2238&langno=2>

6.3 對濫發電郵及惡意程式的防護

6.3.1 濫發電郵

「濫發電郵」是指將大量未經收件人要求而發出的電郵（收件人包括不願接收此類郵件的），例如廣告。濫發電郵會加重網絡負荷，並浪費網絡的頻寬。

學校應考慮安裝過濾濫發電郵的網閘，以過濾所有來自互聯網的濫發電郵，並應定期更新最新的濫發電郵名單／黑名單。學校亦應貯存曾接收過濾濫發電郵的網閘紀錄，以備日後參閱。此外，學校可採納以下保安對策以防止濫發電郵：

- 防止網站撈取電郵地址
- 停止第三者郵件驛遞及不要公開網上代理服務
- 使用公開及私人域名系統(DNS)黑名單以阻止濫發電郵
- 使用許可名單接收郵件
- 利用寄件人的電郵地址、電郵主題或電郵內容過濾郵件，或使用探索法偵測網頁內容過濾技術

附註

學校用戶應遵守以下阻止接收濫發電郵的一般做法：

- 提醒用戶謹慎處理其電郵地址，尤其是填寫網上註冊表格、問卷調查及其他網上文件等；
- 避免向陌生人士及來源發放電郵地址(尤其是作為網站的連結)；
- 在可行的情況下，用戶可使用不同的電郵地址，以免其學校電郵地址及／或電子郵件系統成為濫發電郵的目標；
- 用戶絕對不應以郵件轟炸濫發電郵的寄件人或作出反擊行動；
- 用戶不應回覆濫發郵件，因這樣做只會產生無法傳送的訊息，或讓濫發電郵的寄件人取得一個有效的電郵地址，以作日後繼續濫發電郵之用；
- 用戶亦可使用電郵軟件中的電郵過濾工具來監控濫發電郵。該等工具讓用戶透過設定簡單的過濾規則，便可阻止或阻隔垃圾電郵；
- 用戶可根據互聯網服務供應商設定的程序，向該供應商提出正式投訴並要求跟進。

6.3.2 惡意程式

「惡意程式」泛指一個相當廣泛的軟件威脅範疇，而這些威脅可對電腦或網絡造成損害或不良效果。潛在的損害包括修改數據、毀壞數據、竊取數據、容許未經授權的系統接達、自動彈出不想要的視窗及進行一些用戶不想做的活動。

惡意程式例子包括電腦病毒、網絡蠕蟲、特洛伊木馬程式、邏輯炸彈、間諜軟件、廣告軟件及後門程式。由於該等惡意程式對軟件及資訊處理設施構成嚴重威脅，故需採取預防措施以防止及偵查惡意程式。

傳統上，惡意程式透過兩個主要渠道傳播：

- (a) 透過網絡的數據傳送，或
- (b) 外置式儲存媒體（如可重複寫入光碟、儲存卡或軟磁碟）。

近來，惡意程式的攻擊更趨自動化和先進。新形式的攻擊可以是多種惡意行動的結合。

為防止受到電腦病毒及惡意程式的攻擊，學校應確保已安裝防毒軟件、惡意程式偵查及修復軟件，並確定它們操作正常。學校亦應定期更新病毒標記及惡意程式定義。

另一方面，學校用戶應注意其使用資訊科技的行為。用戶不應轉發任何惡作劇郵件（即由個人惡意地發出與病毒相關但不實的警告／預警），以免進一步擴散。除了倚賴上述的技術監控措施之外，用戶亦應有責任防止電腦病毒及惡意程式的攻擊。

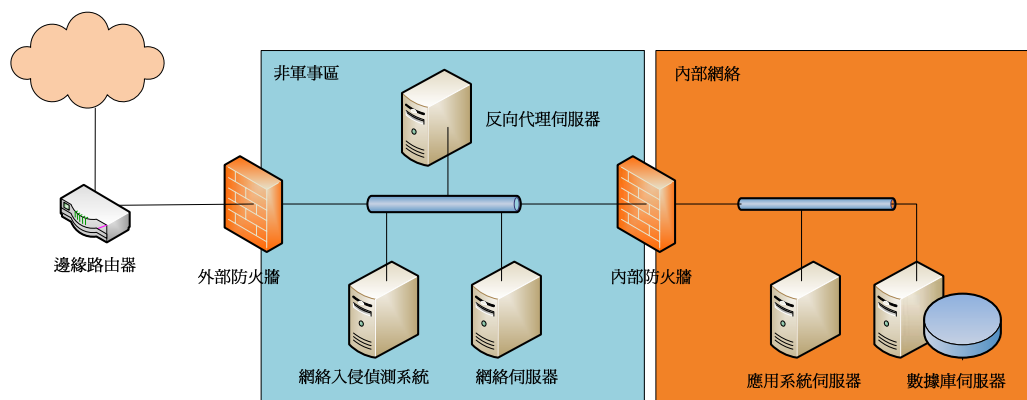
6.4 網絡應用系統保安

雖然網絡應用系統帶來便利與效率，但亦要面對許多保安威脅，因為來自互聯網上任何地方的用戶均可進行接達。這些威脅是源自不可靠的用戶、長期啓用的通訊協議、複雜的網絡技術及不安全的網絡層。

由於網絡技術的複雜性，要進行詳盡的保安分析並不容易亦非簡單。以下章節僅能描述一些較佳的做法作為學校參考資訊。

6.4.1 網絡應用系統保安結構

典型的網上應用系統結構共分三層，結構上把對外網絡伺服器、應用系統伺服器及數據庫伺服器分割排列，如下圖所示。由於這種分層式的結構，即使來自外界的攻擊者已破壞網絡伺服器的防禦，攻擊者仍要尋找其他方法入侵內部網絡。



對外網絡伺服器應限制在非軍事區（DMZ）內。儲存敏感資料的伺服器應設於內部網絡中，並加設額外保護。此外，學校亦應安裝兩堵防火牆，其一可作網絡應用系統的外部防火牆，另一個可作網絡層狀態監測的內部防火牆。兩個防火牆應來自不同的供應商。

其他系統如網絡入侵偵測系統（NIDS）及反向代理伺服器，都應安裝在非軍事區內；該等系統分別用於偵測攻擊，及為用戶提供所有網上應用程式的單一接入點。

至於那些只供內部用戶使用而又未有與外部網絡連結的網絡應用伺服器，學校可考慮實施較少的保安防護措施，例如僅設一層防火牆以分隔網絡伺服器與內部用戶。

建議學校要進行保安風險評估，以確定已實施最合適的保安防護措施。學校亦應注意，要檢查其網絡伺服器以確定伺服器已設定妥當並操作正常。請參閱下表列出的網絡伺服器保安指引：

附註

為提升網絡伺服器的保安效能，學校應遵守以下指引：

- 根據供應商的保安指引，安全地配置網絡伺服器；
- 使用適當的特權賬戶執行網絡伺服器工作。應避免使用特權賬戶，如「root」、「SYSTEM」、「administrator」執行一般網絡伺服器工作；
- 網絡伺服器軟件應採用最新的保安修補程式；
- 設定存取權限，使網絡伺服器軟件不能修改為用戶服務的檔案。換言之，網絡伺服器軟件應只有該等檔案的唯讀權限；
- 在儲存敏感資訊的網絡伺服器內安裝主機入侵偵測系統（HIDS），以監察可疑活動或未經授權而建立／刪除／修改檔案的活動。學校應主動檢視HIDS發出的警告及報告，以便及早識別保安攻擊；
- 設定網絡伺服器軟件以防資料洩漏，如網絡伺服器軟件版本、內部IP網絡地址、目錄架構等；
- 關閉或移除網絡伺服器軟件中不必要的模組；
- 識別網絡伺服器上的應用程式檔案，並以使用權限保護該些檔案；
- 當使用保密插口層時，要為伺服器認證的私人密碼匙備份，並防止它在未經授權的情況下被使用。

6.4.2 網絡應用系統開發程序

倘若網絡應用系統是由學校自行研發或由承辦商開發的，則應在軟件開發的初期階段便考慮下列因素，對網絡應用系統的保安監控作出分析及設定：

- 確保為網絡應用系統設定完備的保安要求；
- 在設計及推行階段應為關鍵的系統進行資訊科技保安風險評估；
- 將保安監控納入系統整合測試及用戶驗收測試中；
- 編製一份保安及質素保證計劃，並採用一些可確保質素的方法，如覆檢編碼、滲透測試及用戶驗收測試等；
- 在啓用系統之先及系統作出重大變動之後，須進行資訊科技保安審查。

軟件開發小組應遵守一套網絡應用安全編碼實務守則，以防禦常見的網絡應用保安漏洞。

有關網絡應用系統安全編碼的資訊，請參閱載於以下網址的「資訊科技保安政策及指引文件編號G3」第10.7.4章節：

<http://www.ogcio.gov.hk/chi/prodev/download/g3.pdf>

6.5 更多資訊

有關網絡和通訊保安的更多資訊，請參閱：

文件名及連結	資料來源
<ul style="list-style-type: none">■ 資訊科技保安指引 (政府資訊科技總監辦公室資訊科技保安政策及指引文件編號G3) http://www.ogcio.gov.hk/chi/prodev/download/g3.pdf	香港特別行政區政府 政府資訊科技總監辦公室
<ul style="list-style-type: none">■ 互聯網通訊保安指引 (政府資訊科技總監辦公室資訊科技保安政策及指引文件編號G50) http://www.ogcio.gov.hk/chi/prodev/download/g50.pdf	香港特別行政區政府 政府資訊科技總監辦公室

7 保安審查及保安事故處理

學校需定期監測及檢視校內所有已設定的保安監控設施。這些審查可確保所有相關保安措施妥善實施，以防保安威脅。

但如上文所述，即使所有保安監控及措施已妥善地實施，亦無法百分百保證資訊科技系統或網絡安全，因此，在真正發生保安事故之前，學校應作好準備。此外，學校亦需確保校內每個用戶知道，當懷疑有問題發生時應聯絡何人。

7.1 保安審查

保安日誌可追蹤及偵測威脅的發生。在學校系統及網絡內的所有活動，一般均可以用日誌紀錄追蹤到。

舉例說，當入侵者闖入學校的學與教網絡時，日誌紀錄會顯示何人曾於何時登入系統，試圖接達某些敏感檔案失敗，試圖執行某些程式等。日誌紀錄亦會顯示於這段期間成功存取及執行的敏感檔案及程式。因此系統管理員便可透過審查日誌，知悉並跟進未經授權的活動。

此外，學校應確保只有獲授權的人士才可存取審查日誌。由於審查日誌連同其他的支援資訊，對於記錄、追蹤及處理保安事故非常重要，因此定期的保安審查是十分重要的。

例子

甲校使用視窗2000作為學校學與教網絡的操作系統。系統管理員使用視窗2000內置的審查功能便可追蹤惡意活動及違反保安事件。

經考慮學校環境後，系統管理員決定採取以下行動：

- 審查試圖「登入賬號」及「存取資料」失敗的事件
- 審查所有系統、應用程式及保安錯誤

系統管理員定期使用相關的審查工具檢視各項記錄。例如，管理員審查日誌紀錄以察看是否發生過多次試圖登入但失敗，以及拒絕存取敏感檔案等事件。

7.2 保安事故處理程序

倘若學校不幸發生保安事故，學校必須妥善地處理。

以下是一些在學校環境中經常出現的保安事故：

常見的資訊科技保安事故	例子
<ul style="list-style-type: none"> ■ 病毒感染 	接收帶有病毒的電郵；使用來源不明的檔案等
<ul style="list-style-type: none"> ■ 與賬戶及密碼有關的事件 	用戶忘記密碼；登入失敗的次數過多而導致賬戶被鎖等
<ul style="list-style-type: none"> ■ 硬件、軟件、數據及資料的損毀／遺失 	電腦故障；硬磁碟故障；遺失軟件媒體；意外刪除檔案等

■ 誤用系統及網絡	安裝未經授權的軟件；惡意變更配置；網絡打印機過多列印工作等
■ 網絡入侵	來自互聯網的駭客入侵；來自校內使用者的網絡攻擊等

不過，學校需注意，不同的事故需要不同的處理程序。在任何情況下，學校應確保校內所有用戶均知道當懷疑有保安事故時應聯絡何人，及懂得如何保護檔案等。

學校需在事故過後進行跟進分析，以檢視保安監控要否作出任何改善。在某些情況下，可能需予以紀律處分。

以下是一些受病毒感染及網絡入侵的保安事故的處理程序例子。雖然這些例子不一定適用於所有學校及所有情況，但學校可一併細閱下一節的參考連結，相信有關資料能幫助學校處理資訊科技保安事故。

7.2.1 例子－處理病毒感染

以下是處理病毒感染的一般指引及程序。當然學校應參閱本身採用的防毒軟件的使用手冊以獲取更多資訊，。

處理病毒感染



■ 第0步 安裝並啟動防毒軟件

如前一章所述，所有電腦系統，包括工作站及伺服器均需安裝防毒軟件。防毒軟件應隨每次開啓電腦系統時啟動，這種安排十分重要，是避免、檢查及清除電腦病毒所必須採取的先決措施。

■ 第1步 隔離受感染系統

當防毒軟件偵測到系統內有病毒或疑似病毒的活動時，會在螢幕上顯示一個訊息，或稱之為病毒警告，這些警告表明學校系統可能已遭到病毒的感染。

建議學校應集中處理事故並停止執行任何其他程式和工作。由於某些電腦病毒會在系統重新啓動時損毀儲存在硬磁碟上的數據，故不應立即關閉或重新啓動已受感染的系統。

若受感染的系統接連着學校網絡，必須盡快隔離有關系統，如拔取網絡電纜以中斷有關的連結。

■ 第2步 通知適當人員並尋求協助

即時通知**適當人員**並尋求協助是非常重要的。一般情況下，學校的系統管理員及／或技術支援服務人員，都可以協助處理病毒感染事故。如有需要，學校亦可考慮尋求保安專家的建議。

■ 第3步 嘗試消滅病毒及修復系統

學校應從防毒軟件提示訊息的指引及程序，小心決定應當採取的選項／行動。

倘若對選項不知如何決定，應立即向技術人員求助，如學校的系統管理員或技術支援服務人員。

若面對一個「修復」（或類似）的選項，「修復」通常是最佳選項，因為它可清除病毒並修復受感染的檔案／項目。

然而，視乎病毒的種類及威力、防毒軟件的版本，以及系統的配置，防毒軟件有時會不能消滅病毒及修復檔案／系統。在這些情況下，學校應仔細考慮採取甚麼適當的行動，有時學校可能需要透過在備份中復原某些檔案以修復系統。

同樣地，若不知如何選擇項目，應向技術人員求助。

■ 第4步 對受感染系統進行病毒防護

學校應透過安裝合適的軟件來防護及改善系統防禦病毒的能力，如使用最新的病毒定義檔及系統／應用軟件的修補程式。

此外，學校需密切監測受感染的系統，以確定它能否恢復運作及病毒是否仍然存在。

■ 第5步 恢復運作並作出檢討

在事故徹底處理及受感染的系統回復至正常的運作模式後，學校須進行一個跟進分析，所有相關人士應開會討論有關事故及曾採取的措施，並從中汲取經驗。

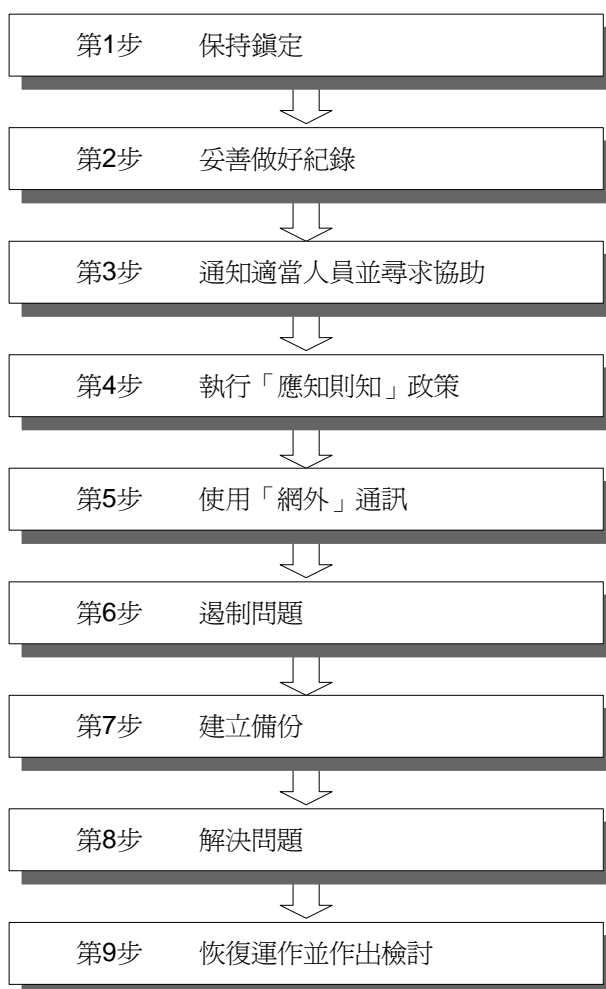
學校應重新評估所有現行的程序及按需要作出修訂，並向相關人員提出建議。學校應確保所有相關的保安監控及措施均是妥善地實施。

本章最後一節列出了一些保安機構及軟件供應商的連結，建議學校定期瀏覽這些網站，以獲取最新病毒警告資訊。

7.2.2 例子－處理網絡入侵

以下是一些處理網絡入侵的一般指引及程序。當中某些步驟對於應用在學校環境來說可能略為嚴謹，但這些步驟都是值得學校一看及作為基本的參考。

處理網絡入侵



■ 第1步 保持鎮定

由於入侵者可能已侵入受損系統數日或甚至數個星期，故再多幾小時其實分別不大。學校應保持鎮定，檢視及考慮一下以下步驟。

■ 第2步 妥善做好紀錄

學校應在發生事故期間作有系統及完整的筆記，當中應記錄：(i)與事故有關的事件發生／被發現時的日期及時間，(ii)受影響的系統、程式或網絡的資料，及(iii)所有對話，包括交談對象、交談日期及時間，以及交談內容如相關的指示。這些記錄及觀察對於檢討溝通及回顧事件至為重要，並可在事件訴諸法庭的情況下作為證據。

■ 第3步 通知適當人員並尋求協助

即時通知**適當人員**並尋求協助是非常重要的。應當以「應知則知」為原則，只通知那些「應知則知」此事故的人員。向無關人士提供不正確的資訊可能會導致不良的後果。若有需要，亦可考慮尋求校外保安專家的建議。此外，學校可指派一位同事協助程序的協調及記錄。

■ 第4步 執行「應知則知」政策

學校在可能的情況下，應把事故詳情告知愈少人愈好。電腦保安事故在早期很容易被誤判，除非有必要作出推斷，否則學校宜保持緘默並盡量避免揣測。此外，學校

應注意不尋常索取資料的情況，拒絕向自稱是保安人員的來電者，透露有關事故的具體資料，如牽涉的賬戶、程式或系統名稱等。

■ 第5步 使用「網外」通訊

學校應避免使用受損系統討論事故的處理，應使用電話及傳真進行聯絡。由於入侵者可能已可以完全地進入受損系統，甚至校內的其他系統（例如電郵系統），因此入侵者可以閱讀郵件訊息及阻截網絡通訊。若必須使用電腦通訊，可考慮使用附有保安措施的隔離系統，例如筆記簿型電腦等，並將所有有關事故處理的郵件加密。

■ 第6步 遏制問題

即使學校管理層可能決定要保持受損系統與網絡的連接，以捕捉入侵者，但校方亦須採取必要的措施防止問題惡化，還要盡快把受損系統從網絡中移除。

以下是一些可能需要採取的行動以遏制問題惡化：

- 若能確定攻擊來源，應阻止可疑人士及網絡連結接達系統
- 考慮將受損系統與外界（如互聯網）及任何其餘網絡中斷連結；尤其須將受感染系統，與敏感資料及要處理緊急任務的系統隔離
- 考慮關閉遙距登入服務，如「rlogin」或「telnet」指令時間
- 考慮關閉程式遙距執行服務，如「rexec」
- 考慮終止所有進行中的可疑處理程序
- 確保只有授權人士獲賦予管理特權

■ 第7步 建立備份

學校應為檔案系統及系統資料建立備份。系統狀態包括網絡連接、臨時檔案及其他易變的數據源（如記憶體內的資料）應轉儲為檔案，然後以檔案系統備份。學校亦須建立多個完整檔案備份（在可能情況下至少使用兩種不同方法），並仔細標籤有關的備份檔案。

■ 第8步 解決問題

學校應找出問題的根源。這並非是一件容易或短時間內做到的事，學校須確定找出讓入侵者有機可乘的漏洞。病毒／蠕蟲感染及駭客／黑客入侵都是常見的保安事故。

以下是一些需要採取的行動以確定問題所在：

- 用最新防毒程式掃描系統
- 檢查系統二進制的完整性
- 檢查所有審查追蹤，包括系統、應用程式以及保安日誌

在確定事故原因及檢查過所有的最新及完好備份之後，學校需以對用戶產生最少影響為原則，利用那些最新及完好備份將系統恢復至安全及正常運作模式。

之後，學校應安裝附有最新修補程式的合適軟件並關閉任何不必要的服務，作好預防及改善系統的防禦能力。學校亦應刪除不再使用的賬戶，並考慮要求用戶重設密碼。

此外，學校應密切監測系統，以確定它能否恢復運作及是否仍存有保安漏洞。

最後，切記在根除問題前保留所有證據，並對學校系統及網絡中的其他系統進行漏洞分析。若未能消除整個網絡的漏洞，必然會引致更多的入侵事故。

■ 第9步 恢復運作並作出檢討

在事故徹底處理及所有系統回復至正常的運作模式後，學校須進行一個跟進分析，所有相關人士應參與會議，對所採取了的措施及汲取了的教訓作出討論。

所有現行的程序應重新評估及在有需要的情況下作出修訂。如有合適建議，應向相關人員闡述。學校應確保所有相關的保安監控及措施均是妥善地實施。

7.3 更多資訊

如想獲取更多有關保安審查及保安事故處理的資訊，可參閱：

文件名稱及連結	資料來源
<ul style="list-style-type: none"> ■ 處理公司的資訊保安事故 http://www.infosec.gov.hk/chinese/sme/management/incident.htm 	香港特別行政區政府
<ul style="list-style-type: none"> ■ Site Security Handbook — 一九九七年九月 (第2196號徵求意見稿) (只有英文版) http://www.ietf.org/rfc/rfc2196.txt 	互聯網工程專責組
<ul style="list-style-type: none"> ■ Incident Handling Procedures (模板) http://www.sans.org/resources/policies/ 	美國系統網絡安全協會

8 用戶關注及教育

有時學校可能只注意安裝及配置適當的硬件和軟件，以保護本身的資訊科技資產，卻忽略了用戶的操作習慣及教育。

然而必須強調，用戶保安意識的教育，實在較前文所述的任何保安監控，更為重要。

8.1 教育至為重要！

倘若用戶未能正確地執行硬件及軟件的預防措施，那些措施便形同虛設。

在前一章所講述的數據保安，不單指出要保護電子資訊，還要保護那些可供授權人士查閱及存取的資訊。學校可使用軟件將檔案加密，並貯存在學校的伺服器中，只容許有存取權的人士使用。然而，學校還應保護重要資訊的印刷本。

因此，除了前文所述的系統及網絡保安措施之外，更重要是提高用戶的保安意識，以及教育他們。

8.2 保護電腦及用戶

伺服器室的閘門及警報系統、硬件上的資產標記、登入密碼、防毒軟件及互聯網通訊閘等保安措施，均為保護學校的資訊科技資產，如硬件、軟件、數據及資訊等。

然而，學校應注意，妥善計劃用戶資訊科技保安的教育，不僅可以保護資訊科技資產，同時亦可保護用戶本人。

8.2.1 例子－用戶在互聯網上的安全

以使用互聯網為例：現今上網已愈來愈見簡單和普及，學生及教師可以很方便地在家中或許多公共設施中（如青少年中心及圖書館等）接觸互聯網上的資訊。

世界上任何人，包括學生、教師、你和我等，都可以在萬維網上發布資訊。然而，沒有人可以完全監控在萬維網上應存放的資訊內容，只能依賴個人的自律，確保其行為是恰當的。

互聯網世界由形形色色的人組成。多數的人是守禮和尊重他人的，但亦有部分是粗魯、冒犯、無禮、甚至刻薄及會利用他人。儘管學校用戶透過上網獲益良多，但他們，尤其是學生，亦可能成為罪案受害者或被人利用的目標。

8.2.2 互聯網上的風險

互聯網上存在若干風險，例如用戶可能會接觸到不恰當的資訊，如色情、厭惡或暴力資訊，亦可能被教唆參與危險或違法的活動。

學生面對的風險尤其顯著，這是因為他們較大可能會參與網上討論（例如，聊天室、ICQ等）這類朋友式交往活動。學生可能會提供一些資料或安排見面，危及他們自身的安全。例如，心懷不軌者可能會利用電郵、公告板或聊天室以獲取年輕學生的信任，然後安排會面。

8.2.3 教育及指引

學校應與家長合作，了解學生的網上活動，並教育用戶如何恰當地使用互聯網及其他系統。讓他們懂得在「虛擬世界」、學校甚至家裏享受由資訊科技帶來快樂、健康、且有益的體驗。

8.3 最佳安排

當學校引入新系統予用戶使用時，應教授他們有關(i)系統使用，及(ii)安全使用的最佳方法。在本文件中所討論的保安監控及措施都要教育用戶及需要他們參與，例如：

- 保護接達及儲存媒體
- 處理密碼
- 防護電腦病毒
- 使用合法及獲授權的軟件及硬件
- 管制軟件的變更
- 阻隔不知名檔案的資源
- 使用電腦的行為守則
- 使用互聯網的道德操守
- 保安意識及處理事故

學校應注意以上僅是部分例子，學校可為用戶教育注入不同或更多主題。本章最後一節列出了一些可供學校作進一步參考的連結，載有一些對學校有用及有幫助的指引，這些指引主要就保護電腦及保護用戶在互聯網上的安全，提供意見。

學校應閱讀這些指引，並因應學校的環境制定合適及所需的保安措施。之後，學校應將這些措施納入本身的用戶教育計劃內，並在推行用戶教育時注意下述各項。

8.3.1 教育方法

其實，學校可以有很多方法教育用戶及提高他們的資訊科技保安意識，例如教師可在學年開始時在電腦課中教育學生。

教師及學校職員可透過參加資訊科技培訓計劃及／或在日常工作中一步步學習，從而掌握資訊科技保安知識。學校亦宜鼓勵他們在校務會議上分享有關經驗。

此外，學校亦可在一些學校活動如早會中，提醒用戶注意資訊科技保安。

8.3.2 義務及責任

學校應強調資訊科技保安的重要性，闡述相關規定及道德操守，並教育用戶正確及負責任地使用學校內的系統及網絡。此外，學校亦應考慮為用戶訂立用戶守則(AUP)。

學校用戶守則是一份訂明用戶使用學校資訊科技設施的「可做」及「不可做」文件。學校可選擇在守則中加入免責聲明，及列出有違保安規定的有關行動。

學校可參考以下的樣本以制定校本用戶守則，學校亦可考慮要求所有用戶在使用學校的資訊科技設施之前，均要閱讀及簽署該份守則。

文件名稱及連結	資料來源
---------	------

<ul style="list-style-type: none"> ■ 資訊科技用戶守則 http://www.hkcampus.net/ser_zone/info/rule.html 	香港資訊校園
<ul style="list-style-type: none"> ■ 用戶守則聲明 (模板) http://www.sans.org/resources/policies/ 	美國系統網路安全協會

8.3.3 推廣及督導

學校應向用戶推廣及提醒他們有關資訊科技保安對學校的重要性。

為方便查閱有關的資訊，學校可考慮把用戶守則視為公開資料，並在學校的公共區域中宣傳推廣，例如把用戶守則張貼在走廊、圖書館及電腦室的公告板上，掛貼在公用電腦資訊站上，及／或上載至學校網頁中（如有）。

學校應緊記，儘管已推行資訊科技保安教育，並且已獲用戶承諾有良好的行為，但監督方面仍是不可忽視的。當學生於圖書館及電腦室使用電腦時，教師仍必須在場監督與指導。

8.4 更多資訊

以下連結是為學校提供更多有關資訊科技保安用戶教育的資訊，部分資訊更可用作為基礎用戶教育的參考資料。

文件名稱及連結	資料來源
<ul style="list-style-type: none"> ■ 青少年資訊保安認知簡介 http://www.info.gov.hk/digital21/chi/ecommerce/pki/wbt/flash/ITSecuWBT.html 	香港特別行政區政府 數碼21資訊科技策略
<p>How to keep your child safe on the Internet (只有英文版) http://www.info.gov.hk/police/hkp-home/english/tcd/csnet.pdf</p>	香港特別行政區政府 香港警務處（防止罪案科）
<ul style="list-style-type: none"> ■ 小型電腦系統保安手冊 http://www.info.gov.hk/police/hkp-home/chinese/tcd/Chinese%20CS%20Handbook.pdf 	香港特別行政區政府 香港警務處（防止罪案科）
<ul style="list-style-type: none"> ■ Using the Internet and Technology in the Classroom (只有英文版) http://www.ehhs.cmich.edu/~tvantine/edint.html 	Education Central

此外，一些組織以及政府的政策局及部門，會不時為學生及教師舉辦資訊科技保安講座或培訓計劃。學校應瀏覽那些組織及部門的網站，並搜尋該些活動的有關資訊及報名詳情。

主頁

- 教育局資訊科技教育組
<http://www.edb.gov.hk/ited>

- 香港教育城
<http://www.hkedcity.net/>

- 香港個人資料私隱專員公署
<http://www.pcpd.org.hk/cindex.html>

- 數碼21 資訊科技策略—中學學生資訊保安認知講座
http://www.info.gov.hk/digital21/chi/pastevents/isas_sss.html

9 資訊科技保安政策

在閱讀前文之後，學校應能理解資訊科技保安的基本知識。為使學校所有系統、網絡、用戶及管理均符合已計劃／採用的保安措施，學校應考慮制定一套**資訊科技保安政策**。

9.1 甚麼是資訊科技保安政策？

資訊科技保安政策是一套政策及程序指引，說明在各項保安監控中所要採取的保安措施。例如在實體保安方面，學校應制訂校內的保安區域，以及有關保護流動裝置、存取及儲存媒體的指引。

此外，學校亦可制訂密碼處理、預防電腦病毒、互聯網的恰當使用及防護措施等指引、以及遇上事故時的聯絡資料，其他保安監控中使用系統及網絡的守則等文件。

9.1.1 擬定政策

沒有一套資訊科技保安政策適用於所有學校。學校應閱讀本文件內的有關資訊，再因應本身的獨特環境而確立相關的保安要求，從而選定適當的保安級別並寫下在各項保安監控中所應採取的措施。

學校可參考本章最後一節的文件連結，以擬定校本資訊科技保安政策。

9.1.2 系統配合

學校的系統及網絡配置應能反映學校所制定的政策。

倘若政策規定用戶密碼必須每60天更改一次，學校的系統管理員便應在學校系統的配置上作出配合，用戶亦應遵守該政策，並監察任何例外的情況。

如前文所述，學校可以使用一些內置的管理工具（如微軟視窗XP、NT 4.0及／或視窗2000系統專用的強制漫遊設定檔、「域用戶管理器」、「系統原則編輯器」、群組原則等）以及附加工具（如Internet Explorer管理員工具包、保安顧問／檢驗員），令保安設定變得容易。

在某些情況下，學校可能會覺得要制定一些保安政策，以能配合學校系統的目標，是一件困難的事。為讓政策發揮效用，學校必須尋求一個適當的平衡，避免過分謹慎或寬鬆。

9.1.3 教育及推廣

學校必須教育所有用戶，包括學生、教師、學校員工、系統管理員及管理層，遵守學校所制定的政策及程序。

此外，所有用戶應可取閱有關的政策文件。學校可考慮將該文件張貼在走廊、電腦室及課室的報告板上，並將文件存放於學校網站及／或檔案伺服器的公共區域中。

儘管學校會認為保安程序降低了用戶操作的靈活性，並增加管理工作，但適當地制定校本資訊科技保安政策是非常重要的。

9.1.4 審查及檢討

學校必須對用戶遵守資訊科技保安政策進行定期的審查。此外，亦要定期檢討有關的政策及程序，以切合學校需求的改變，以及適應環境及科技的變遷。

9.2 更多資訊

其他有關資訊科技保安政策的資訊，可參閱下列文件。學校可參考並採用文件相關部分以擬定校本資訊科技保安政策。

文件名稱及連結	資料來源
<ul style="list-style-type: none"> ■ Standards and Guidelines for Strategic Systems (只有英文版) http://www.wits2.murdoch.edu.au/security/sg-strategic.html ■ Standards and Guidelines for Desktop Computers (只有英文版) http://www.wits2.murdoch.edu.au/security/sg_desktops.html 	梅鐸大學 (Murdoch University, 澳洲)
<ul style="list-style-type: none"> ■ A Short Primer For Developing Security Policies (只有英文版) http://www.sans.org/resources/policies/Policy_Primer.pdf 	美國系統網絡安全協會

10 結語

資訊科技保安對學校十分重要。由於在學校應用資訊科技的情況日益廣泛及複雜，為保護學校的資訊科技設施，學校及學校用戶在計劃、設計、部署及使用學校系統及網絡時，應謹記**三個保安目標**。

此外，在學校環境中共有**六種常見的保安監控**。學校要在這些監控中採取合適級別的保安措施，並就學校的獨特環境考慮其他保安問題。

最後，資訊科技保安涉及技術、操作及管理等問題，讓資訊科技保安成為學校文化是很重要的。學校應將各項保安監控中所採取的保安措施化成條文，制定**資訊科技保安政策**，以便要求所有用戶遵守。