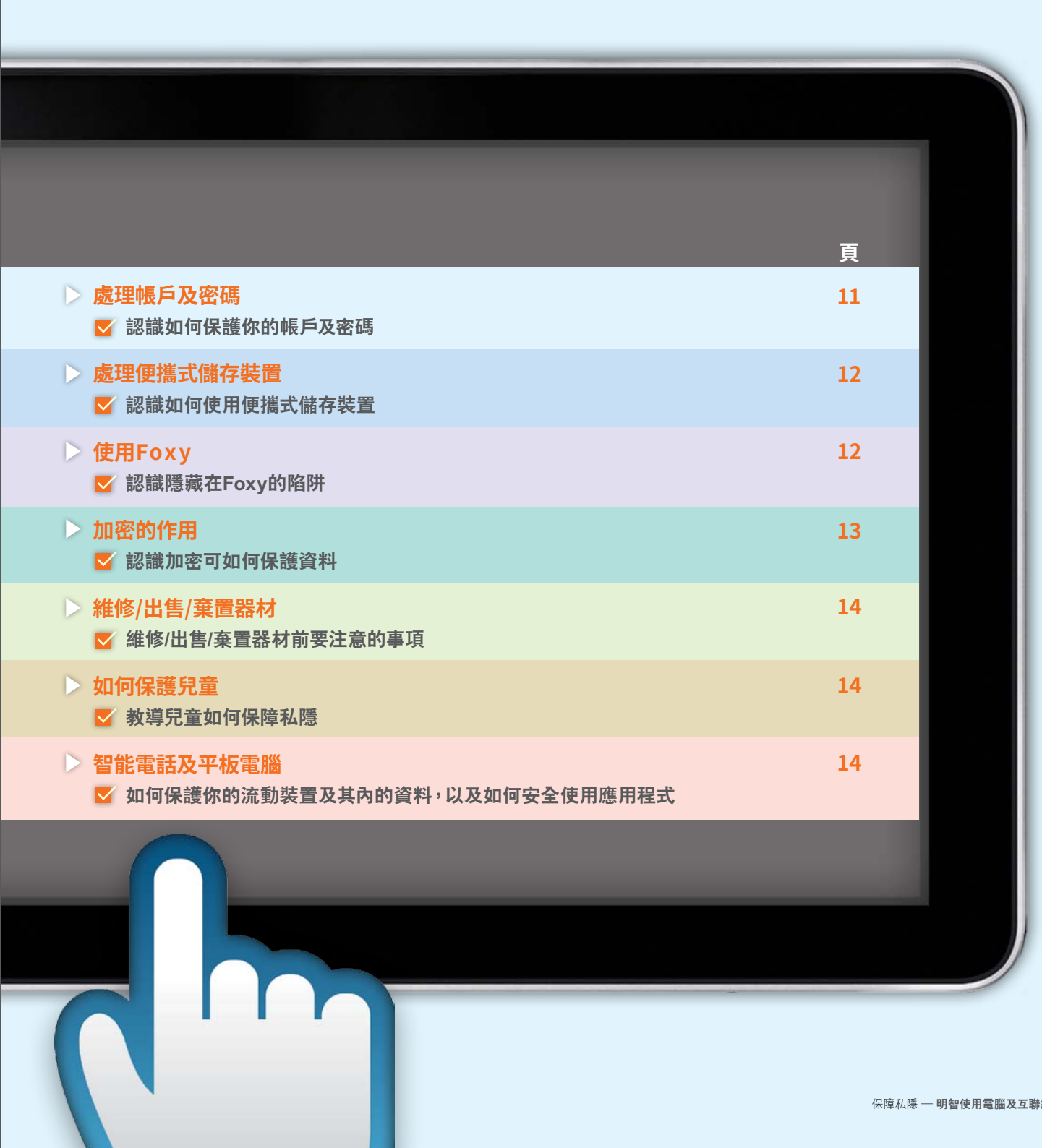
香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

保障私隱 —
明智使用電腦及互聯網

注意清單

使用電腦或互聯網前，請留意以下事項：



保障私隱 — 明智使用電腦及互聯網

本小冊子提供有關使用資訊及通訊裝置時如何保護個人資料的實用貼士及建議。

確保資訊及通訊裝置的安全

第一道防線是要確保上網裝置（例如電腦、智能電話及平板電腦）的安全。
下述的保安步驟可減低你的裝置受惡意軟件侵害的風險：

安裝適當的防毒軟件

- 惡意軟件是病毒、蠕蟲、特洛伊木馬[1]、鍵盤記錄[2]、殭屍[3]等程式的統稱，可以損害你的電腦及／或盜取你的資料。請安裝最新的防毒軟件（付費或免費皆可），並根據軟件商的建議，定期更新病毒數據檔案。
- 市場上亦有適合用於智能電話及平板電腦的防毒軟件可供使用。由於這些流動裝置已普及成為上網的用具，而其儲存個人資料的容量可媲美電腦，以防毒軟件加以保護這些裝置尤其重要。
- 如你的作業系統或防毒軟件設有個人防火牆，你應開啟個人防火牆。個人防火牆可以控制裝置的網絡通訊及減少系統被黑客入侵或攻擊的風險。

1. 特洛伊木馬是宣稱做某事，但暗地裏亦做其他事的程式，例如作為鍵盤記錄器、檔案分享器及／或殭屍。
2. 鍵盤記錄程式可捕捉你的按鍵，包括網址、用戶名稱及密碼，在你不知情下將該等資料發送予黑客。
3. 殭屍程式可以控制你的電腦，在你不知情下讓黑客遙距地發送垃圾郵件、攻擊網站等。

以用戶而不是管理員的身份登入

- 安裝防毒軟件並不是防禦所有惡意軟件的萬全方法。另一個有效保護電腦的方法是在日常的使用中只採用「用戶模式」。當你以管理員的權限登入電腦，任何惡意軟件一旦成功進入你的電腦就可自行安裝。請為你自己及其他使用你的電腦的人士開立「用戶模式」帳戶（即不可安裝軟件的帳戶），以防禦惡意軟件。此外，有很多資訊，例如到訪網站紀錄、曾瀏覽網頁、用戶名稱及密碼，都會儲存於帳戶內。如你不想其他人看到這些資訊，請開立不同的用戶帳戶，以確保有關資訊只限於相關用戶查閱。

啟動安全更新

- 請經常為你的裝置的作業系統進行安全及版本更新。很多惡意軟件會利用作業系統的漏洞進行破壞。更新你的作業系統是堵塞此等風險的良好方法。

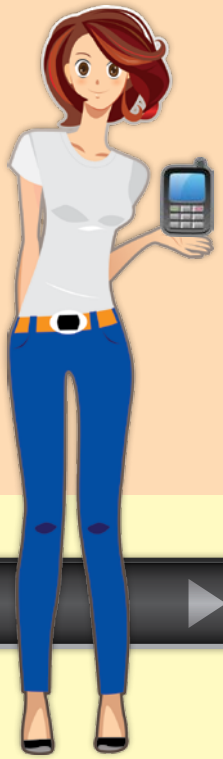
切勿安裝盜版軟件

- 幾乎所有盜版軟件及其下載網站都含有惡意軟件。因你需要以管理員的身份登入電腦以便安裝盜版軟件，惡意軟件就可當成盜版軟件的一部分而自行安裝。防毒軟件並非一定能偵測出所有惡意軟件。因此，到訪盜版網站、下載及／或安裝盜版軟件、音樂或視像，都會帶來極大的風險。
- 請謹記，世上沒有免費午餐。免費下載原本需要付費的軟件、音樂或視像，一定帶有風險，不如你想的美。

資訊及通訊裝置的實體保安

實體的保安工作可以保護被遺留或遺失的裝置，避免內載的資料被取閱。

把不使用的裝置鎖上



- 智能電話及平板電腦：應時刻使用密碼屏幕鎖，以防止其他人在未經你准許的情況下使用。
- 電腦：除了設定登入密碼外，你應使用密碼保護屏幕程序，令其他人不能在沒有你准許的情況下使用你的電腦。

安裝防盜軟件

- 請考慮安裝防盜軟件，萬一你的裝置被遺失或盜去，你可以追蹤裝置的下落。有些防盜軟件可以讓你在屏幕上顯示訊息，警告拾取裝置的人，或容許你遙距刪除裝置內的所有資料。

在網上提供個人資料前要三思

要確認在網上要求你提供個人資料的人士的身份是非常困難的。一個精明的網友，要懂得質疑網站為何要收集它所要求的個人資料。提防虛假的電郵及網站。

你的個人資料一旦在網上流傳或洩露，基本上是沒法阻截的，故此在網上披露個人資料前應該三思並考慮其後果。

要清楚知道向誰人及為何提供個人資料

- 你同意向要求你提供個人資料的人提供資料前，請三思。想一想他們向你索取的每項個人資料是否有真正的需要。
- 在提供你的朋友或親屬的個人資料以換取優惠前，請三思。易地而處，想一想你會希望你的朋友或親屬如何保護及尊重你的個人資料。
- 向網站或經電郵提供個人資料前，想一想你是否真正知道你在向誰提供資料。合法的網站可輕易被複製，而虛假的網站也可看似非常專業及真實。

要明白披露個人資料會帶來的影響

- 在社交網站張貼個人資料前，請三思。資料一旦在網上披露，你就無法阻止它在網上被傳閱及搜索到。請細閱個人資料私隱專員公署發出的《在網絡世界保障私隱－精明使用社交網》[4]單張。
- 你在某個網站上披露的無傷大雅的資訊，例如寵物名字，可能是你在其他網站用作重設密碼的安全提示問題。請三思選擇披露該些資訊及小心選擇重設密碼問題。

你是否被要求提供超乎適度的資料?

- 問一問自己，網站或其他資料使用者在網上要求的個人資料就收集目的而言是否超乎適度。舉例說，如網站只想確定你不低於可以使用該網站的年齡，為何需要你提供出生年月日？同樣地，如你不是購買貨品，為何網站需預先要求你提供信用卡號碼及／或住址？
- 切勿為了優惠而提供個人資料。想一想對方或會將該資料作甚麼用途。例如，對方可能會用以對你的喜好作分析，甚至詐騙活動。

4. *見：http://www.pcpd.org.hk/chinese/publications/files/SN_c.pdf*

提供個人資料前細閱《收集個人資料聲明》及《私隱政策聲明》

- 《收集個人資料聲明》述明你是否必須提供你的個人資料、收集資料的目的、資料承轉人的類別，以及為查閱及改正你的個人資料時，你可以聯絡的人士。
- 《私隱政策聲明》述明該機構的私隱政策及實務措施。《私隱政策聲明》涵蓋的範疇一般會超越資料的收集，包括該機構會如何處理、使用及保留其持有的個人資料。

不要輕信非預期收到的電郵訊息

- 電郵訊息可以是虛假的，而發件人亦可以是偽冒的。因此在回應電郵要求前，請三思。如非預期的電郵要求你登入網上銀行、付款、電郵、社交網絡等服務，切勿按電郵內的任何連結。你應使用你的瀏覽器上的標籤連結。如有關訊息屬實，你以自己的已定標籤登入這些服務後，應該可以看到同樣的要求。
- 同樣地，當你收到一些並非預期的電郵，不應開啓內裏的附件。

上網的安全

要懂得安全地連接Wi-Fi無線網絡

虛假的Wi-Fi網絡熱點易被設置。若你使用這些虛假的網絡熱點傳輸通訊，你的個人資料有可能被截取。此外，透過未經加密的Wi-Fi網絡傳遞的通訊亦可以被其他連接至該Wi-Fi網絡的器材接收。以下的Wi-Fi網絡通訊措施可助減低使用Wi-Fi網絡時的風險。

- 當你使用公共 Wi-Fi 上網時，請時刻確保你不是以管理員的身份登入你的電腦，以減低被惡意軟件破壞的風險。
- 不論你是否使用公共 Wi-Fi，當透過 Wi-Fi 瀏覽含敏感資料網站（電子銀行、電郵、社交網站、網上購物等）時，請時刻確保你已採用 SSL（詳見下文）加密通訊，以免你的資料被截取。
- 在設定家居 Wi-Fi 時，請時刻以 WPA 或 WPA2 加密技術來保護你的資料。使用公共 Wi-Fi（例如政府 Wi-Fi）時，如有提供的話，請時刻連接至經 WPA 或 WPA2 加密的接入點。

要懂得安全地使用公共電腦

因為無法確保公共電腦是否曾被改動，所以不應使用公共電腦收發敏感資料或個人資料。

- 切勿使用公共電腦瀏覽含敏感資料網站（電子銀行、電郵、社交網站、網上購物等），因為你不知道這些電腦有沒有被安裝惡意軟件，例如鍵盤記錄程式。使用保安程度不詳的公共電腦會增加披露你的個人資料予不明人士的風險。

不要讓裝置記錄你的登入狀態

「記錄我的登入狀態」的設定可使你的電腦的瀏覽器記錄你於網站的用戶名稱及密碼，以便你日後瀏覽同一網站時不需再重新登入。雖然這功能提供了方便，但它也讓任何能使用你的電腦的人皆可登入你的帳戶。

- 如你並非使用你的私人電腦瀏覽網站，請不要在「記錄我的登入狀態」一欄加上剔號。

使用保密插口層(SSL)來保護訊息

SSL是瀏覽網站所使用的加密技術。如你到訪的網址是以「https://」而非「http://」開首，那麼有關通訊已受SSL加密保護，以防被竊取。如你使用Wi-Fi上網，這個做法尤其重要，因為很多Wi-Fi設施是沒有啟動基本加密的。

- 在網上提供任何敏感個人資料（例如信用卡號碼）予可以信賴的網站前，請確定該網站的網址是以「https://」開首。當使用「https://」開啟網站時，瀏覽器亦會同時檢查網站的身份。你可以從瀏覽器上的說明找到如何利用顯示於屏幕的掛鎖或鑰匙圖像來辨明網站的身份。
- 你可以在很多普及的電郵和社交網站啟動自動的「https://」連接。如可能的話，好好利用這方法。請在相關網站查看如何啟動「https://」。當啟動後，這些服務的流動程式中的通訊，也會受加密保護。

認識網站Cookies

Cookies是你到訪過的網站在你的電腦中儲存的檔案。它可以載有你的喜好、購物車的選擇，及／或你的瀏覽歷史。Cookies可分不同種類，有些是瀏覽網站必須的，有些只是為了追蹤你的網絡行為而設。你需要對cookies有基本認識以便知道如何選擇接受或拒絕它們。

- Cookies 有不同的種類。很多需要用戶登入的網站須使用 Session（工作階段）cookies，它們讓你無需在每一頁輸入用戶名稱及密碼。在你關閉瀏覽器時，session cookies 即被刪除。為此，你應考慮接受 session cookies，否則當你瀏覽這些網站時，會遭到拒絕。

- 另一種是持久 cookies。即使你已關閉瀏覽器，持久 cookies 仍然留在電腦內。第一方持久 cookies 載有你的喜好或與你到訪的網站有關的瀏覽活動。你可以選擇接受或拒絕接受它們，但拒絕接受它們或會令你無法瀏覽某些網站或某些部分。如你拒絕接受此類 cookies，網站應會告訴你是否仍可使用該網站。

- 第三方持久 cookies 多是網上廣告公司在你瀏覽的網站購買了「位置」而擺放的。如你不希望被第三者追蹤，你應拒絕第三方 cookies。這不應影響你的瀏覽情況。你應查看你的瀏覽器，了解如何拒絕接受第三方 cookies。

- 有些網站則採用其他技術，例如 Flash cookies。這些 cookies 不會理會瀏覽器的設定而停留在你的電腦內的。如你已安裝最新版本的 Acrobat Flash，你可設定控制板上的 Flash Player，拒絕接受 Flash cookies。製造此類「超級／殭屍 cookies」（不理會用戶設定及難以移除的 cookies）的技術日新月異。如你擔心你的網絡行為會被追蹤，應定期在互聯網上了解這課題的最新發展。

- 很多瀏覽器設有「私人／安全模式」。在這模式下，只要你關閉瀏覽器，瀏覽器便應該不會留下瀏覽的蹤跡（即不會保留瀏覽、表格或下載紀錄、緩存檔案、儲存的密碼等），並拒絕接受 cookies。不過，這模式保障私隱的程度因瀏覽器而異。你在依賴瀏覽器的保障之前，應了解其保障程度。另外，使用「私人／安全模式」或會減慢你的瀏覽速度，因為瀏覽器不會記錄你曾到訪的網頁或你的喜好。

處理帳戶及密碼

認識如何保護你的帳戶及密碼

如果你在多個帳戶使用同一帳戶名稱及密碼的組合，一旦密碼外洩或被猜中，便會使多個帳戶同時受被入侵的威脅。由於很多網站容許使用者利用登記的電郵地址來登入，即使你使用同一電郵地址去在多個網站登記不用的帳戶，只要黑客取得係電郵地址的登入密碼，便可利用同一電郵地址及密碼入侵你的帳戶。

同樣地，如果你在多個網站使用同一帳戶名稱或登記電郵，其他人就可把你在這些網站上的資料及身份串連起來。

- 請建立一套更改密碼的方法讓你能在不需書寫的情況下仍可記起更改後的密碼。請不要在多個帳戶使用同一密碼，特別是一些存有敏感資料的帳戶。
- 切勿以相同的名稱開立多個網上帳戶或以相同的電郵地址登記多個帳戶。
- 請使用最少由八個數字及字母組成的複雜密碼或按照網站提示的密碼複雜性去訂立密碼。
- 不要披露你的密碼予任何人（包括聲稱代表該網站的人）。如果你懷疑你的密碼已被洩露，你應盡快更改所有使用這密碼的帳戶密碼。

處理便攜式儲存裝置

認識如何使用便攜式儲存裝置

便攜式儲存裝置指 USB 記憶體、平板電腦、手提電話或其他可攜帶的儲存裝置。你須考慮一旦遺失此類便攜式儲存裝置的後果。

- 因為這些裝置可以很容易被遺失，請時刻為便攜式儲存裝置內的資料備份。
- 請時刻把便攜式儲存裝置內的檔案加密（有關如何把檔案加密，詳見下文）。沒有解密密碼的人便不能解讀其中的資料。

使用Foxy

認識隱藏在Foxy的陷阱

很多 Foxy 的版本會在你不知情下自動啓動並分享你的整個硬碟，故使用 Foxy 危險重重。檔案一旦經 Foxy 被分享，便無法阻止它散播開去。

- 由使用 Foxy 而導致的資料外洩事件發生了很多次，當中用戶並不知道 Foxy 將其敏感資料與他人分享。在使用 Foxy 前，你應問問自己，是否真正知道 Foxy 如何運作及如何設定它。
- 由於製造 Foxy 的供應商已結業，現已沒有下載 Foxy 的可靠來源。因此，你應問問自己可以如何肯定你所下載的 Foxy 複本沒有被篡改或受惡意軟件感染。

加密的作用

認識加密可如何保護資料

如你的電腦被黑客入侵或當你遺失便攜式儲存裝置，加密是防止當中資料被解讀的有效方法。謹記要為加密用的密碼作出有效的保護措施，包括不要把它與被加密的電腦或便攜式儲存裝置存放在一起。

- 現時有很多方法及軟件程式（收費及免費）讓你把電腦及便攜式儲存裝置（包括智能電話）內的檔案加密。你應熟悉最少一種加密檔案的方法。例如：

  - 你可以使用免費及多重平台的開放源碼軟件TrueCrypt (www.truecrypt.org)，在硬盤或USB記憶體內開立一個「儲物箱」，內裏儲存的所有檔案會被加密。
  - 如果需要為獨立檔案加密，你可以安裝7-Zip (www.7-zip.org) 作加密的工具。它亦是一個免費及多重平台的開放源碼軟件，可以壓縮檔案及文件夾，並同時支援加密。

- 你需要採用強效「加密算法」，例如 “AES”。以 TrueCrypt 開立「儲物箱」或以 7-Zip 加密檔案時，請確保你已選擇這加密算法。

- 如你需以電郵發送個人資料，在發送前應把個人資料儲存於檔案中，然後加密。將檔案加密除可保障個人資料在傳輸時的安全，亦可保障資料免在接收端外洩（例如，接收資料的電腦被黑客入侵或檔案被 Foxy 或其他分享軟件不經意地分享）。你不應以電郵發送加密密碼。以其他途徑發送加密密碼可防止檔案及密碼同時落入他人手上（例如錯誤輸入收件人的電郵地址）。

維修/出售/棄置器材

維修/出售/棄置器材前要注意的事項

很多人可能沒有意識到儲存於電腦或便攜式儲存裝置內的個人資料的豐富程度。由於你或不能移除或刪除載有資料的儲存裝置，如沒有在棄置、出售或送予第三者前採取適當的保護措施，你便可能將自己的個人資料送予他人。

- 你應確保你所選的維修商信譽可靠。把資料交託維修商前，你應確保你滿意其保障個人資料的承諾。
- 如你需要把電腦或具有可移除的儲存裝置的器材送往維修，而問題與儲存裝置無關，你應先把儲存裝置移除。如你必須把儲存裝置送往維修，可能的話，應先以安全及永久的方法（例如硬盤適用的DBAN (www.dban.org)或檔案適用的FileShredder (www.fileshredder.org)）把所有個人資料刪除。
- 同樣地，如你準備出售或棄置具有記憶或儲存功能的裝置，切記刪除內裏的所有資料。有些裝置的生產商，例如流動電話生產商，會提供刪除電話內所有資料的步驟。你應依從這些步驟。切記移除或刪除這些裝置內的記憶卡或舊有的SIM卡。

如何保護兒童

教導兒童如何保障私隱

兒童可能未完全意識互聯網及資訊科技隱藏的陷阱對他們的私隱的影響。他們需要盡早認識如何保護自己。

- 請與你的子女討論本冊子內的建議可如何協助他們在使用互聯網時保護其個人資料。教導他們一旦其個人資料在網上發佈或洩漏，這些資料便可能永遠留存在互聯網上。

智能電話及平板電腦

若要認識如何在使用智能電話或平板電腦時保護自己的個人資料，包括如何保護你的流動裝置及其他的資料，以及如何安全使用應用程式，請參閱《保障私隱-明智使用智能電話》[5]單張。

5. *http://www.pcpd.org.hk/chinese/publications/files/smartphones_smart_c.pdf.*

香港個人資料私隱專員公署

查詢熱線：(852) 2827 2827
傳真：(852) 2877 7026
地址：香港灣仔皇后大道東248號12樓
網址：www.pcpd.org.hk
電郵：enquiry@pcpd.org.hk

網上私隱要自保專題網站

www.pcpd.org.hk/besmartonline

版權

如用作非牟利用途，本小冊子可部分或全部翻印，但須在翻印本上適當註明出處。

免責聲明

本小冊子所載的資料只作一般參考用途，並非為《個人資料(私隱)條例》(下稱「條例」)的應用提供詳盡指引。有關法例的詳細及明確內容，請直接參閱條例的條文。個人資料私隱專員(下稱「專員」)並沒有就上述資料的準確性或個別目的或使用的適用性作出明示或隱含保證。上述建議不會影響專員在條例下獲賦予的職能及權力。

© 香港個人資料私隱專員公署

2014年4月（第一修訂版）