規章

蒙郡公立學校

相關條目: BBB, EDC, EDC-RA, EGI-RA, EHC-RA, IGS, JFA, JFA-RA, JHF-RA, JOA-RA, KBA-RB**,** KBB
責任辦公室: Superintendent of Schools

電腦系統、電子資訊和網路安全的用戶責任

I. 目的

A. 確保蒙郡公立學校(MCPS)電腦系統、相關科技和電子資訊所有要素的安全

B. 為 MCPS 電腦系統的所有用戶說明哪些是適當的使用;

C. 通過在安全的環境裡使用電腦系統、相關科技和電子資訊促進智力發展; 並

D. 確保符合州、地方和聯邦的相關法律規定。

II. 背景

MCPS 因著符合 MCPS 使命的用途為學校和學生提供電腦設備、電腦服務和網絡連接。供 MCPS 用戶使用的各種大量資訊技術帶來了新的風險和機遇。展現適當行為的責任落在使用 MCPS 資訊科技資源和電腦設施的所有人身上。在學校，未成年人的上網活動由工作人員通過全系統的技術保護措施進行監督。將根據工作、職責和是否需要知情提供訪問級別。用戶必須保護資訊和資源免遭盜竊、惡意破壞、未經授權的使用、篡改或丟失。

III. 定義

A. *獲准的電子簽名方式*是指由教育總監和/或其指定負責人根據本規章及所有相關州法和聯邦法律批准的方式, 這種方式明確了電子簽名的形式、與電子簽名同時使用的系統和規程、以及使用電子簽名的重要性。

B. *電腦系統*是指硬件、軟件和相關技術, 包括網絡、線路和通訊設備。

C. *網絡霸凌和/或電子騷擾或恐嚇*是指使用電子通訊(包括電子郵件、即時短訊、社交網站、博客、手機或其它技術手段)並通過嚴重妨礙學生教育福祉、機會或學業表現、或學生身體或心理健康而營造敵意教育環境的故意行為, 而且:

- 行為的動機是出於實際存在或被認為存在的個人特性，包括種族、原屬國籍、婚姻狀況、性別、性取向、性別認同、宗教、血統、身體特徵、社會經濟地位、家庭狀況、身體或精神殘疾
- 行為具有威脅或嚴重恐嚇性質
- 行為發生在學校物業中、學校活動中、或在校車上
- 行為嚴重擾亂學校的正常運作

D. *教育目的*是指直接促進 MCPS 教育、教學、行政、業務、和支持服務使命的行動, 並且與用戶負責的任何教學、項目、工作、工作分配、任務或職能有關。

E. *電子數據和資訊*是指任何電子或數碼形式的事實或數字。範例包括電子郵件、即時短訊、聊天室、短信、文件、數據庫、檔案、網站、以及以電子形式儲存的其它任何資訊。

F. *電子記錄*是指以電子形式產生、發送、接收和儲存、與 MCPS 業務行為有關、在當事方之間交流並作為交易證據、且為 MCPS 記錄用途而保存的資訊。記錄不包括性質過於短暫以至於通常不予保存的資訊。

G. *電子簽名*是與電子記錄附在一起或有邏輯相關性、且由有意簽署該記錄的人執行或採納的電子聲音、符號或過程。

H. *不當材料*是指具有淫穢或黃色性質且因此傷害未成年人/學生的材料, 包括在本規章中說明的與成人/色情內容有關的網站、不適合年齡的材料、不具備教育目的的材料、或不符合系統安全或 MCPS 政策和規章的材料。不當材料還可能包括宣傳或推進黑客、使用、散發和生產毒品、酒精和菸草、霸凌、騷擾和恐嚇、犯罪技能、暴力或非法使用或持有武器的材料。如果工作人員確定需要進行真正的研究或其他合法目的，則可以授予適當的使用權。

I. *網絡連接*包括用來連接到網絡伺服器和用戶的所有獲得授權的方式, 以及所有獲得授權的提供連接的方式。

J. *技術保護措施*是一種網絡過濾技術, 根據旨在限制或防止獲得不當材料的規定條件限制進入網絡的某些部分。

K. *未經授權的設備*是指沒有得到技術總長辦公室(OCTO)和/或其指定負責人批准用來連接 MCPS 電腦或 MCPS 網絡的任何設備, 包括但不僅限於電腦、平板設備、個人通訊和管理設備(例如無線熱點)、智能手機或手機; 遊戲設備; 攝影設備; 以及娛樂設備(例如 MP3 遊戲機或 iPods™)。

L. *用戶*是指 MCPS 的任何工作人員、學生或被授權使用 MCPS 電腦系統的其他個人。其他個人可能包括家長、義工和合同工或臨時工。

IV. 規程

以下章節說明電子數據和資訊安全、電子交易和簽名、實體安全、系統和應用程式安全、網絡安全、及行為和使用方面網絡安全和網絡道德的必要規程。在 MCPS 網站上公布的 ***MCPS** 電腦系統安全程序手冊*將介紹更多有關電腦系統安全的具體用戶責任和規程。

A. 電子數據和資訊安全

用戶只能獲取和進入他們獲得授權且工作和職責所需的資訊和/或電腦系統。

1. 用戶對自己個人的帳戶負責。

   a) 用戶必須按照要求更改密碼, 並對密碼嚴格保密。

   b) 明確禁止用戶共用帳戶和密碼。

   c) 能夠被追查到個人帳戶名的任何違規行為將被視為帳戶所有人的責任。

2. 在離開電腦或工作台或允許他人使用前, 用戶必須退出所有系統。

3. 每個用戶都有責任了解和遵守符合本規章的安全規程。

4. 用戶必須保證自己的電子數據的安全。(說明: 敏感文件必須保存在安全的地方, 例如個人的網絡檔案夾/目錄或移動磁盤, 然後把磁盤鎖在文件櫃裡)。
5. MCPS 對由於系統故障或中斷而可能丟失的資訊概不負責。用戶應當製作備份並確保把備份保存在安全的地方。

B. 電子交易和簽名

當馬里蘭州法、聯邦法律或 MCPS 政策或規章要求一項交易必須有授權人的簽名時, 如果電子記錄與使用獲准電子簽名方式所做的電子簽名有關, 即被視為符合這項要求。授權及使用電子交易和簽名的規程在 ***MCPS*** *電腦系統安全程序手冊*中說明。

C. 實體安全

電腦系統設備必須放置和保存在一個安全的實體環境中。用戶有責任遵守電腦和相關技術的實體安全條例。

1. 當工作人員不在現場監督時, 放置貴重電腦設備的所有區域(包括固定或臨時倉庫)都必須上鎖。

2. 在沒有適當授權的情況下不得把電腦或相關設備帶離 MCPS 物業。

3. 用戶必須採用各自工作場所的問責規程簽入或簽離任何電腦或相關設備。用戶在離開 MCPS 或調到另一所學校或辦公室前必須把這個設備歸還給對其擁有所有權的學校、部門或小組。

4. 將盡可能準確地保存工作場所的設備庫存。在購買後, 設備將被添加到庫存清單中。用戶不得拆除電腦上的庫存標誌或標籤。

5. 丟失和被盜的設備應當依照 MCPS 規章 EDC-RA, *家具和設備庫存控制*的規定進行處理。

D. 系統和應用程式安全

1. 根據 ***MCPS*** *電腦系統安全程序手冊*的陳述, 在未經相關人員許可的情況下, 用戶不得因任何目的安裝軟件或硬件, 或關閉或修改在任何電腦或其它經授權的數碼/電子設備上安裝的安全設定或措施(例如防病毒軟件)。

2. 根據 *MCPS 電腦系統安全程序手冊*的陳述, 在未經相關人員許可的情況下, 用戶不得更改系統設置。
3. 不得在非 MCPS 的電腦上安裝或複製 MCPS 的軟件和應用程式, 許可證協議明確規定的情況除外。

E. 網絡安全

所有對 MCPS 網絡和信息的訪問都必須獲得 MCPS OCTO 的授權人員批准。如果被認為危害網絡或獲取信息時違反了這項或其它任何的 MCPS 相關政策或規章, 用戶的帳戶或訪問可能會被刪除、暫停或取消。

F. 行為和使用

將通過多種方式監督學生和教職員使用互聯網的情況, 包括但不僅限於技術和直接監督。

1. 用戶負責確保訪問或輸入網絡上的材料是出於在本規章中闡述的教育目的。

2. 有意張貼或從 MCPS 系統或互聯網站連接的任何材料或信息都必須符合本規章闡述的教育目的。

3. 用戶將負責遵守適用於他們所用電腦系統的制度, 包括從 MCPS 設備提供的互聯網上訪問的系統。

4. MCPS 不能控制也無法對通過 MCPS 訪問的其它系統或互聯網站上存儲的信息負責。MCPS 以外的一些網站和系統可能會含有誹謗、不準確、侮辱、淫穢、褻瀆、性導向、威脅、種族冒犯、或非法的材料。

5. 根據 III.D 一節的說明, 電腦設施、網絡和其它科技資源只能用作教育目的, 所有使用行為都可能被 MCPS 審查, 而且可以被記錄和存檔。

6. MCPS 電子郵件僅供教育目的使用。所有活動都受 MCPS 的審查, 並且可以被記錄和存檔。所有學生使用 MCPS 電子郵件必須獲得授權, 以便支持和促進學習流程。

7. 禁止學生使用未獲授權的電子郵件、即時短訊或聊天室。

8. 雖然不可能記錄所有不當的行為和對電腦設施的不當使用, 但是, 以下準則提供了禁止使用電腦和網絡的違規範例:

a) 破壞系統(也被稱作黑客)或通過提供如何破壞 MCPS 任何系統(任何未經授權對操作系統、個人帳戶、網絡共享文件夾、軟件、網絡設施和/或其它程序進行修改)的指示或信息, 協助他人造成破壞和/或破壞設備。

b) 使用硬件設備或軟件程式解密密碼、按鍵記錄或未經授權記錄密碼、以及/或未經授權訪問更高級別的信息或特權或嘗試這樣做。

c) 故意妨礙其他用戶使用網絡或電腦, 例如通過拒絕服務(DoS)或分布式拒絕服務(DDoS)。

d) 發表中傷他人、誹謗性或構成網絡霸凌、騷擾或恐嚇他人的言論或行動。

e) 故意訪問或嘗試訪問不當材料(如以上 III. H.所述)。

f) 引入造成損壞或破壞 MCPS 電腦系統預期功能的惡意編碼/軟件(例如病毒或蠕蟲)。

g) 在未獲得 OCTO 和/或指定負責人授權的情況下把未經授權的設備連在任何 MCPS 電腦或 MCPS 網絡上。

h) 使用電子郵件在互聯網上發送具有威脅性質或未經請求的批量和/或商業消息來騷擾或欺騙他人, 或為了盜竊身份而使用欺騙性電子郵件獲取個人信息。

i) 通過使用代理、應用程式或其它方式規避技術保護措施(也被稱為網絡安全或過濾技術)。

j) 未經許可而刪除、偽造、修改、讀取或複製其他用戶的電子郵件或嘗試這樣做。

k) 未經教育總監和/或其指定負責人授權而讀取、刪除、複製、轉發、打印、分享或修改其他用戶的數據文件。

l) 允許他人使用自己個人的 MCPS 電子郵件地址、帳戶或密碼。

m) 允許他人使用自己個人的 MCPS 網絡帳戶、網絡文件夾或密碼。

n) 在 MCPS 系統上使用商業廣告、連鎖信或非教育性質的遊戲。

o) 未經授權而複製或傳送受版權保護的材料和軟件。

p) 使用 MCPS 設備或資源通過電子方式在互聯網上張貼或散播未經授權的可識別個人信息, 或張貼有關學生或教職員的虛假信息。

q) 使用 MCPS 網絡或電腦系統謀取個人利益或從事任何犯罪活動。

9. 所有用戶不得故意參與未經授權地披露、使用和散播有關未成年人的個人信息。

10. 應當教育學生適當的在線行為, 包括與他人在社交網絡網站和聊天室的互動, 以及認識網絡霸凌和回應。

11. 發現互聯網某個部分含有沒有被技術保護措施過濾掉的不當材料的 MCPS 電腦系統的任何用戶必須而且應當遵循 *MCPS 電腦系統安全程序手冊*闡述的規程, MCPS 的網站提供這本手冊。

V. 違反規章

A. 違反本規章中陳述的規程和標準將受到紀律處分。

1. 對員工的紀律處分可能包括開會、警告、批評信、失去優惠權、停職停薪、降職、解職和/或刑事指控。

2. 對學生的紀律處分可能包括但不僅限於致電家長或監護人; 失去優惠權、賠償、停學和/或開除; 以及/或刑事指控。(參見 MCPS 規章 JFA-RA, *學生權利和責任*和學校的處分政策。)

3. 對其他用戶的紀律處分可能包括失去優惠權和/或刑事指控。

B. MCPS 電腦系統的任何用戶應當舉報可疑或不當的數據使用、濫用電腦系統、或可能的安全漏洞。駐學校的用戶應當通知校長或負責資訊技術的校長指定

負責人。非駐學校的用戶應當通知直接主管和教育總監和/或其指定負責人。在 *MCPS 電腦系統安全程序手冊*中闡述的嚴重違規行為還應當向 OCTO 報告。

規章發展史: 新規章, 1995 年 8 月 22 日; 1999 年 12 月 13 日修訂; 2000 年 6 月 1 日更新辦公室名稱; 2002 年 6 月 10 日修訂; 2007 年 5 月 23 日修訂; 2012 年 7 月 27 日修訂。