QUY ĐỊNH

CÁC TRƯỜNG CÔNG LẬP QUẬN MONTGOMERY

Mục Liên Quan: BBB, EDC, EDC-RA, EGI-RA, EHC-RA, IGS, JFA, JFA-RA, JHF-RA, JOA-RA, KBA-RB, KBB

Văn Phòng Trách Nhiệm: Giám Đốc Các Trường Học

Trách Nhiệm Khi Xử Dụng Hệ Thống Máy Điện Toán Và Sự An Toàn Của Hệ Thống

I. MỤC TIÊU

A. Để đảm bảo an ninh cho tất cả các yếu tố của hệ thống máy tính, công nghệ liên quan và thông tin điện tử của các Trường Công Lập Quận Montgomery (MCPS);

B. Để phân định các phương cách sử dụng phù hợp cho tất cả những người dùng hệ thống máy tính MCPS;

C. Để thúc đẩy phát triển trí tuệ thông qua việc sử dụng các hệ thống máy tính, công nghệ liên quan và thông tin điện tử trong một môi trường an toàn; và

D. Để đảm bảo tuân thủ luật pháp tiểu bang, địa phương và liên bang.

II. BỐI CẢNH

MCPS cung cấp máy móc điện toán, dịch vụ điện toán, và sự truy cập mạng lưới cho các trường học và học sinh với mục tiêu kiên định với nhiệm vụ của MCPS. Nhiều thông tin kỹ thuật dành cho những người xử dụng MCPS đưa đến các nguy cơ và cơ hội mới. Trách nhiệm đối với hành vi phù hợp thuộc về tất cả các cá nhân sử dụng tài nguyên công nghệ thông tin và cơ sở máy tính MCPS. Tại trường học, các sinh hoạt trên mạng của các trẻ em được nhân viên kiểm soát qua những biện pháp bảo vệ toàn hệ thống kỹ thuật. Mức độ truy cập được cung cấp tùy thuộc vào sự phân công, trách nhiệm và sự cần thiết để biết. Những người xử dụng phải bảo vệ những thông tin và phương sách để tránh việc bị trộm, phá hoại, xử dụng không phép, giả mạo, và mất mát.

III. ĐỊNH NGHĨA

A. Một *phương pháp chữ ký điện tử được chấp thuận* là đã được giám đốc của các trường và/hoặc người được chỉ định chấp thuận, theo quy định này và tất cả các luật liên bang và tiểu bang hiện hành, và định rõ quy định hình thức chữ ký điện tử,

hệ thống và thủ tục được sử dụng với chữ ký điện tử, và ý nghĩa của việc sử dụng chữ ký điện tử.

B. Một *hệ thống máy tính* là phần cứng, phần mềm và công nghệ liên quan, bao gồm mạng, hệ thống dây điện và thiết bị truyền thông.

C. *Bắt nạt trên mạng và/hay quấy nhiễu hoặc đe dọa qua hệ thống điện tử* có nghĩa là hành vi cố ý sử dụng giao tiếp điện tử như e-mail, tin nhắn tức thời, trang xã hội, blog, điện thoại di động hoặc các phương pháp công nghệ khác để tạo ra một môi trường giáo dục hận thù bằng cách quấy rầy đáng kể vào lợi ích, cơ hội hay thành tích học vấn của học sinh hay với sức khỏe thể chất hay tâm lý của học sinh, và là:

- Được thúc đẩy bởi một đặc điểm cá nhân thật sự hay cảm nhận, bao gồm chủng tộc, nguồn gốc quốc gia, tình trạng hôn nhân, giới tính, định hướng tình dục, nhận diện về giới tính, tôn giáo, nguồn gốc, đặc điểm thể xác, hoàn cảnh kinh tế xã hội, tình trạng gia đình, hay khả năng hay khuyết tật về thể chất hay tinh thần; hay

- Mang tính đe dọa hay dọa dẫm nghiêm trọng

- Xảy ra tại khuôn viên trường học, tại các hoạt động hay sự kiện do trường bảo trợ, hay trên xe buýt trường học; hay

- Xáo trộn trật tự điều hành của trường một cách đáng kể

D. *Mục đích giáo dục* là những hành động trực tiếp thúc đẩy các nhiệm vụ giáo dục, hướng dẫn, hành chính, kinh doanh và dịch vụ hỗ trợ của MCPS và liên quan đến bất kỳ hướng dẫn, dự án, công việc, phân công công việc, nhiệm vụ hoặc chức năng nào mà người dùng chịu trách nhiệm.

E. *Dữ liệu và thông tin điện tử* là những sự kiện hoặc số liệu trong bất kỳ hình thức điện tử hoặc kỹ thuật số. Ví dụ bao gồm e-mail, tin nhắn tức thời, phòng trò chuyện, nhắn tin, tài liệu, cơ sở dữ liệu, hồ sơ, trang mạng và bất kỳ thông tin được lưu trữ điện tử nào khác.

F. Một *hồ sơ điện tử* là thông tin được tạo, gửi, nhận hoặc lưu trữ ở dạng kỹ thuật số liên quan đến hoạt động kinh doanh MCPS, được truyền đạt giữa các nhóm như là bằng chứng của giao dịch và được lưu giữ cho mục đích tài liệu MCPS. Một hồ sơ không bao gồm thông tin có tính chất tạm thời mà nó không được bảo tồn thông thường.

G. Một *chữ ký điện tử* là một âm thanh, biểu tượng hay quá trình điện tử, được gắn vào hoặc liên kết hợp lý với một hồ sơ điện tử và được thực hiện hoặc chấp nhận bởi một người có ý định ký một hồ sơ.

H. *Các vật liệu không thích hợp* là những tài liệu tục tĩu hoặc khiêu dâm và do đó có hại cho các em vị thành niên/học sinh, bao gồm các trang mạng liên quan đến nội dung người lớn/quan hệ tình dục, tài liệu không phù hợp với lứa tuổi và tài liệu không có mục đích giáo dục, như được định nghĩa trong quy định này hoặc không phù hợp với hệ thống an ninh hay chính sách và quy định an toàn MCPS. Các tài liệu không phù hợp cũng có thể bao gồm những tài liệu thúc đẩy hoặc thúc đẩy xâm nhập, sử dụng, phân phối và sản xuất ma túy, rượu và thuốc lá, bắt nạt, quấy rối và đe dọa, kỹ năng phạm tội, bạo lực hoặc sử dụng hoặc sở hữu vũ khí trái phép. Trong trường hợp nhu cầu nghiên cứu thực sự hoặc mục đích hợp pháp khác được xác định bởi nhân viên, có thể được cấp quyền truy cập phù hợp.

I. *Truy cập internet* bao gồm tất cả các phương thức được phép sử dụng để kết nối với nơi phát hiện Internet và người xử dùng và tất cả các phương thức được phép để cung cấp quyền truy cập.

J. Một *biện pháp bảo vệ công nghệ* là một công nghệ lọc Internet được thiết kế để giới hạn quyền truy cập vào các phần được chọn của Internet dựa trên các tiêu chuẩn đã xác định được thiết kế để giới hạn hoặc ngăn chặn sự truy cập vào tài liệu không phù hợp.

K. *Thiết bị trái phép* là bất kỳ thiết bị nào không được Office of the Chief Technology Officer (OCTO) và/hoặc người được chỉ định để kết nối với máy tính MCPS hoặc hệ thống mạng MCPS, bao gồm, nhưng không giới hạn ở các máy tính, thiết bị máy tính bảng, giao tiếp cá nhân và tổ chức các thiết bị như điểm truy cập không dây, điện thoại cầm tay hoặc điện thoại di động; thiết bị trò chơi; thiết bị chụp ảnh; và các thiết bị giải trí như máy nghe nhạc MP3 hoặc iPod.

L. Một *người dùng* là bất kỳ nhân viên MCPS, học sinh hoặc cá nhân nào khác được phép sử dụng các hệ thống máy tính của MCPS. Các cá nhân khác có thể bao gồm cha mẹ, tình nguyện viên, và nhân viên thầu hoặc nhân viên tạm thời.

IV. PHƯƠNG THỨC

Phần sau đây mô tả các quy trình cần thiết cho an toàn mạng, an ninh mạng và an ninh mạng về bảo mật dữ liệu và thông tin điện tử, giao dịch và chữ ký điện tử, bảo mật vật lý, bảo mật hệ thống và ứng dụng, an ninh mạng và cách cư sử và sử dụng. Các trách nhiệm và quy trình cụ thể hơn của người dùng đối với bảo mật hệ thống máy tính được nêu trong *Hướng Dẫn về Quy Trình Bảo Mật Hệ Thống Máy Tính MCPS* có trên trang mạng MCPS.

A. Bảo Mật Dữ Liệu và Thông Tin Điện Tử

Người dùng chỉ có thể truy cập thông tin và/hay hệ thống máy tính mà họ được ủy quyền và cần cho các bài tập và trách nhiệm của họ.

1. Người dùng chịu trách nhiệm cho các tài khoản cá nhân của riêng họ.

    a) Người dùng phải thay đổi mật khẩu theo yêu cầu và giữ kín mật khẩu.

    b) Người dùng tuyệt đối bị cấm chia sẻ tài khoản và mật khẩu.

    c) Bất kỳ vi phạm nào có thể bắt nguồn từ tên tài khoản cá nhân sẽ được coi là trách nhiệm của người chủ tài khoản.

2. Người dùng phải đăng xuất khỏi tất cả các hệ thống trước khi rời khỏi máy tính hoặc trạm làm việc hoặc cho phép người khác sử dụng nó.

3. Đây là trách nhiệm của mỗi người dùng để nhận thức và tuân theo các quy trình an toàn theo quy định này.

4. Người dùng phải giữ an toàn các dữ liệu điện tử của họ. (Lưu ý: Các hồ sơ nhạy cảm phải được lưu vào một vị trí an toàn, chẳng hạn như hệ thống thư mục cá nhân/mục lục hoặc một đĩa di động được giữ kín trong tủ hồ sơ khóa.)

5. MCPS không chịu trách nhiệm về thông tin có thể bị mất do lỗi hệ thống hoặc gián đoạn. Người dùng nên tạo bản sao và đảm bảo giữ các bản sao này ở một nơi an toàn.

B. Giao Tác Điện Tử và Chữ Ký

Trường hợp luật pháp tiểu bang Maryland, luật liên bang hoặc chính sách hoặc quy định MCPS đòi hỏi sự giao tác phải có chữ ký của người được ủy quyền, điều kiện đó được đáp ứng khi hồ sơ điện tử được liên kết với chữ ký điện tử bằng phương pháp chữ ký điện tử được chấp thuận. Các quy trình ủy quyền và sử dụng các giao tác và chữ ký điện tử được nêu trong *Hướng Dẫn về Quy Trình Bảo Mật Hệ Thống Máy Tính MCPS*.

C. Hoạt Động An Ninh

Thiết bị hệ thống máy tính phải được đặt và bảo trì trong một môi trường an toàn. Người dùng có trách nhiệm tuân theo các quy định bảo mật vật lý cho máy tính và công nghệ liên quan.

1. Khi nhân viên không có mặt để giám sát khu vực, tất cả các khu vực (bao gồm lưu trữ vĩnh viễn hoặc tạm thời) thiết bị máy tính có giá trị phải được bảo đảm.

2. Máy tính hoặc thiết bị liên quan không được rời khỏi tài sản MCPS mà không có phép thích hợp.

3. Người dùng phải sử dụng các thủ tục trách nhiệm địa phương để đăng nhập hoặc đăng xuất bất kỳ máy tính hoặc thiết bị liên quan nào. Thiết bị này phải được trả lại cho trường, văn phòng, bộ phận hoặc đơn vị sở hữu trước khi người dùng rời MCPS hoặc chuyển đến trường hoặc văn phòng khác.

4. Việc kiểm kê thiết bị địa phương sẽ được duy trì chính xác khi có thể. Thiết bị sẽ được cộng thêm vào bản kiểm kê khi mua được. Người dùng không được xóa các dấu hiệu hàng kiểm kê hoặc thẻ khỏi máy điện tính.

5. Thiết bị bị mất và bị đánh cắp nên được thi hành theo MCPS Regulation EDC-RA, *Control of Furniture and Equipment Inventory*.

D. Bảo Mật Hệ Thống và Ứng Dụng

1. Người dùng không được cài đặt phần mềm hoặc phần cứng, hoặc phá hỏng hoặc sửa đổi các cài đặt hoặc biện pháp bảo mật (như phần mềm chống vi-rút) được cài đặt trong bất kỳ máy tính hoặc thiết bị kỹ thuật số/điện tử được ủy quyền nào cho bất kỳ mục đích nào mà không có sự cho phép của nhân viên phù hợp, như được nêu trong *Hướng Dẫn về Quy Trình Bảo Mật Hệ Thống Máy Tính MCPS*.

2. Người dùng không được thay đổi cài đặt hệ thống mà không có sự cho phép của nhân viên phù hợp, như được nêu trong phần *Hướng Dẫn về Quy Trình Bảo Mật Hệ Thống Máy Tính MCPS*.

3. Phần mềm và ứng dụng MCPS không được cài đặt hoặc sao chép vào máy điện tính không phải của MCPS, trừ khi được quy định trong thỏa thuận cấp phép.

E. Hệ ThốngAn Ninh

Tất cả quyền truy cập vào mạng MCPS và thông tin cần có sự chấp thuận từ cơ quan có thẩm quyền MCPS trong OCTO. Tài khoản người dùng hoặc quyền truy cập có thể bị lấy đi, đình chỉ hoặc thu hồi nếu được xác định sư truy cập mạng hoặc thông tin được sử dụng vi phạm điều này hoặc bất kỳ chính sách hoặc quy định MCPS hiện hành nào khác.

F. Cách Cư Xử và Sử Dụng

Việc sử dụng Internet của học sinh và nhân viên sẽ được theo dõi bằng nhiều phương pháp bao gồm, nhưng không giới hạn ở công nghệ và giám sát trực tiếp.

1. Người dùng có trách nhiệm đảm bảo rằng việc truy cập hoặc nhập tài liệu trên mạng là cho mục đích giáo dục như được định nghĩa trong quy định này.

2. Bất kỳ tài liệu hoặc thông tin nào được đăng hoặc liên kết có chủ đích từ hệ thống MCPS hoặc trang Mạng phải phù hợp với mục đích giáo dục, như được định nghĩa trong quy định này.

3. Người dùng có trách nhiệm tuân thủ các quy tắc áp dụng cho (các) hệ thống máy tính mà họ sử dụng, bao gồm cả các quy tắc được truy cập qua Internet từ thiết bị MCPS.

4. MCPS không có quyền kiểm soát và không thể chịu trách nhiệm về thông tin trên các hệ thống hoặc trang mạng Internet khác mà có sự truy cập qua MCPS. Một số trang mạng và hệ thống bên ngoài MCPS có thể chứa nội dung phỉ báng, không chính xác, lạm dụng, tục tĩu, thô tục, tình dục, đe dọa, xúc phạm chủng tộc hoặc tài liệu bất hợp pháp.

5. Tất cả việc sử dụng các thiết bị máy tính, mạng và các tài nguyên công nghệ khác phải là cho mục đích giáo dục, như được định nghĩa trong Section III.D., và phải được MCPS xem xét và có thể được ghi lại và lưu trữ.

6. MCPS e-mail chỉ dành cho mục đích giáo dục thôi. Tất cả các hoạt động đều được MCPS kiểm soát và có thể được ghi xuống và duy trì. Tất cả học sinh sử dụng e-mail MCPS phải được phép cho các mục đích hỗ trợ hoặc tạo điều kiện cho quá trình học tập.

7. Học sinh bị cấm sử dụng trái phép e-mail, nhắn tin tức thời hoặc phòng trò chuyện.

8. Mặc dù không thể ghi lại tất cả các hành vi không phù hợp và sử dụng các thiết bị máy tính, các hướng dẫn sau đây cung cấp các ví dụ về các vi phạm sử dụng máy tính và hệ thống mạng bị cấm:

a) Việc giả mạo hệ thống (còn được gọi là xâm phạm) hoặc hỗ trợ người khác tạo sự giả mạo bằng cách cung cấp hướng dẫn hoặc thông tin về cách giả mạo bất kỳ hệ thống MCPS nào (bất kỳ sự thay đổi trái phép nào của hệ thống điều hành, tài khoản cá nhân, thư mục chia sẻ mạng, phần mềm, phương tiện mạng và/hay các chương trình khác) và/hay thiết bị hư hại .

b) Giải mã mật khẩu, khóa đăng ký, hay chiếm giữ mật khẩu trái phép bằng cách sử dụng các thiết bị phần cứng hoặc ứng dụng phần mềm, và/hay đạt quyền truy cập hoặc đặc quyền cấp cao trái phép hay cố gắng làm như vậy.

c) Can thiệp một cách có chủ ý với hệ thống truy cập mạng của những người dùng khác hoặc sử dụng máy tính như qua từ chối dịch vụ (DoS) hoặc từ chối dịch vụ phân tán (DDoS).

d) Đưa ra những phát biểu hoặc hành động phỉ báng, vu khống hay cấu thành đe doạ trực tuyến, quấy rối hoặc đe dọa người khác.

e) Cố ý truy cập hoặc cố gắng truy cập tài liệu không phù hợp, như được xác định trong III. H. trên.

f) Giới thiệu các mã hiểm độc/phần mềm độc hại như vi-rút hoặc sâu gây hại hoặc phá hoại chức năng dự định của hệ thống máy tính MCPS.

g) Gắn thiết bị trái phép vào bất kỳ máy tính MCPS hoặc mạng MCPS nào mà không có sự cho phép của OCTO và/hay người được chỉ định.

h) Sử dụng e-mail để quấy rối hoặc lừa gạt người khác bằng cách gửi tin nhắn hàng loạt và/hay tin nhắn thương mại qua Internet, hoặc sử dụng tin nhắn e-mail lừa đảo để lấy thông tin cá nhân cho mục đích đánh cắp danh tính.

i) Các biện pháp bảo vệ công nghệ tuần hoàn, còn được gọi là công nghệ lọc hoặc bảo mật mạng, thông qua việc sử dụng proxy, ứng dụng hoặc các phương pháp khác.

j) Xóa, giả mạo, sửa đổi hay đọc hay sao chép mà không có phép e-mail của người dùng khác hoặc cố gắng làm như vậy.

k) Đọc, xóa, sao chép, chuyển tiếp, in, chia sẻ hoặc sửa đổi các hồ sơ dữ liệu của người dùng khác mà không có phép của giám đốc các trường học và/hay người được chỉ định.

l) Cho phép người khác sử dụng một địa chỉ e-mail MCPS cá nhân, tài khoản hoặc mật khẩu.

m) Cho phép người khác sử dụng một tài khoản hệ thống mạng cá nhân MCPS, thư mục mạng hay mật khẩu.

n) Sử dụng quảng cáo thương mại, chuỗi thư hoặc các trò chơi không là giáo dục trên các hệ thống MCPS.

o) Sao chép hoặc chuyển giao các tài liệu và phần mềm có bản quyền mà không được phép.

p) Đăng lên Internet hoặc phổ biến bằng phương tiện điện tử thông tin nhận dạng cá nhân mà không được phép hoặc đăng thông tin sai lệch về học sinh hoặc nhân viên, sử dụng thiết bị hoặc tài nguyên MCPS.

q) Sử dụng mạng MCPS hoặc hệ thống máy tính cho ích lợi cá nhân hoặc bất kỳ hoạt động bất hợp pháp nào.

9. Tất cả người dùng đều bị cấm tham gia vào việc tiết lộ, sử dụng và phổ biến trái phép thông tin cá nhân của các em trẻ.

10. Học sinh phải được giáo dục về hành vi trực tuyến phù hợp bao gồm các tương tác với các cá nhân khác trên các trang mạng xã hội và trong các phòng chat, và về nhận biết bắt nạt và phản ứng trên mạng.

11. Bất kỳ người dùng hệ thống máy tính MCPS nào xác định một phần Internet có chứa tài liệu không phù hợp chưa được lọc qua biện pháp bảo vệ công nghệ là phải và dự kiến sẽ tuân theo các quy trình như được nêu trong*Hướng Dẫn về Quy Trình Bảo Mật Hệ Thống Máy Tính MCPS* mà có trên trang mạng MCPS.

V. KHÔNG TUÂN THỦ

A. Việc không tuân thủ các quy trình và tiêu chuẩn nêu trong quy định này là nguyên nhân thích hợp cho hành động kỷ luật.

1. Các hành động kỷ luật đối với nhân viên có thể bao gồm một hội nghị, cảnh báo, thư khiển trách, mất đặc quyền, tạm ngưng việc mà không trả tiền, giáng chức, sa thải, và/hay truy tố tội phạm.

2. Các hành động kỷ luật đối với học sinh có thể bao gồm, nhưng không giới hạn ở một cuộc gọi điện thoại cho phụ huynh hay giám hộ; mất đặc quyền, bồi thường, cấm học và/ hay đuổi học; và/hay truy tố tội phạm. (Xem MCPS Regulation JFA-RA, *Student Rights and Responsibilities,* và các chính sách kỷ luật trường học.)

3. Các hành động kỷ luật đối với người dùng khác có thể bao gồm mất đặc quyền và/hoặc truy tố tội phạm.

B. Bất kỳ người dùng hệ thống máy tính MCPS nào phải báo cáo việc sử dụng dữ liệu nghi ngờ hoặc không phù hợp, lạm dụng hệ thống máy tính hoặc vi phạm an ninh. Người dùng tại trường nên thông báo cho hiệu trưởng hoặc người được chỉ định chịu trách nhiệm về kỹ thuật thông tin. Người dùng không ở trong trường nên thông báo cho người giám sát trực tiếp của họ và tổng giám đốc của trường và/hay người được chỉ định. Những vi phạm nghiêm trọng, như được quy định trong *Hướng Dẫn về Quy Trình Bảo Mật Hệ Thống Máy Tính MCPS*, cũng cần được báo cáo cho OCTO.

Lịch sử Quy luật: Quy luật Mới, Ngày 22 tháng 8, 1995; kiểm lại vào Ngày 13 tháng 12, 1999; cập nhật tên văn phòng Ngày 1 tháng 6, 2000; kiểm lại Ngày 10 tháng 6, 2002, kiểm lại Ngày 23 tháng 5, 2007; kiểm lại Ngày 27 tháng 7, 2012.