

규정/REGULATION MONTGOMERY COUNTY PUBLIC SCHOOLS

관련 항목: BBB, EDC, EDC-RA, EGI-RA, EHC-RA, IGS, JFA, JFA-RA, JHF-RA, JOA-RA, KBA-RB, KBB

책임 사무실: Superintendent of Schools

컴퓨터 시스템과 통신망 보안에 관한 사용자의 의무 (User Responsibilities for Computer Systems and Network Security)

I. 목적

- A. Montgomery County Public Schools(MCPS) 컴퓨터 시스템, 관련 테크놀로지, 전자 정보의 모든 요소의 보안을 확실하게 하기 위한 것입니다.
- B. MCPS 컴퓨터 시스템의 모든 사용자의 적절한 사용을 기술하기 위한 것입니다.
- C. 안전한 환경에서 컴퓨터 시스템, 관련 테크놀로지, 전자 정보의 사용을 통해 지적 개발을 육성하기 위한 것입니다.
- D. 해당하는 주, 카운티 및 지역, 연방법에 따도록 하기 위한 것입니다.

II. 배경

MCPS는 MCPS의 교육 목표에 맞는 목적을 위하여 컴퓨터 장비, 컴퓨터 서비스, 통신망 접속을 학교와 사무실에 제공합니다. 폭넓은 다양한 정보기술은 MCPS 사용자에게 새로운 기회뿐만 아니라 위험요소와도 접할 기회가 됩니다. 적절하게 행동할 책임이 MCPS 정보 테크놀로지 리소스와 컴퓨터 시설을 사용하는 모든 사람에게 있습니다. 학교에서 미성년자의 온라인 활동을 교육구 기술보호조치에 따라 모니터링합니다. 학과 과제, 책임, 알아야 할 필요성에 따라 접속 범위를 제공합니다. 사용자는 정보와 자원을 도난, 악의적 훼손, 권한 밖의 접속, 변경과 분실로부터 보호해야 합니다.

III. 정의

- A. *승인된 전자 서명의 사용(approved electronic signature method)*은 이 규정과 전자 서명에 관한 모든 해당 주와 연방 법, 전자 서명의 사용 시스템과 절차, 전자 서명 사용의 의미에 따라 교육감/대리인의 승인을 통해 사용됩니다.
- B. *컴퓨터 시스템(computer system)*은 하드웨어, 소프트웨어, 네트워크, 와이어, 커뮤니케이션 도구 등을 포함한 관련 테크놀로지를 의미합니다.
- C. *사이버 불링과/또는 온라인에서의 희롱, 협박(Cyberbullying and/or electronic harassment or intimidation)*이란, 이메일, 인스턴트 메시지, 소셜사이트, 블로그, 휴대전화 또는 기타 테크놀로지적 방법과 같은 전자 커뮤니케이션을 사용하여 학생의 교육적 혜택이나 기회 및 수업 이행을 심하게 방해하거나 학생의 신체적 심리적 안녕을 침해하는 것이며 또한 다음과 같은 경우에 의해 행해지는 것을 의미합니다:
- 언어, 신체, 문자, 전자 커뮤니케이션 행위 또는 인종, 국적, 결혼 신분, 성별, 성적 경향, 성별 구분, 종교 및 지체 부자유, 가족의 상태, 신체 또는 정신적 능력 또는 장애 등과 같은 실제 또는 추정된 개인 특징을 협박하거나 심하게 괴롭히는 의도적 언어, 신체적, 문자 및 전자 커뮤니케이션 행위
 - 협박 또는 심각하게 겁을 주는 행위
 - 학교 공공건물, 학교 활동, 학교 통학버스에서 일어났을 경우
 - 학교 운영에 심각하게 혼란을 줄 경우
- D. *교육적 목적(Educational purposes)*은 MCPS의 교육, 교습, 행정, 업무, 도움 서비스와 사용자의 책임이 동반하는 교습, 프로젝트, 직업, 업무, 작업/과제 또는 기능을 직접적으로 육성하는 행동입니다.
- E. *전자 데이터와 정보(Electronic data and information)*는 전자 또는 디지털 형태의 사실 또는 형상입니다. 예로는 이메일, 전자문자, 채팅방, 텍스트링, 서류, 데이터 베이스, 파일, 웹사이트와 전자 상으로 저장한 정보를 포함합니다.
- F. *전자 기록(electronic record)*은 MCPS 업무 실시와 연결되어 형성, 송신, 수신, 저장한 정보로 업무자 간의 업무에 관한 의사소통, MCPS의 기록 보존의 목적으로 유지되는 정보입니다. 기록은 일반적으로 보관하지 않는 일시적인 성격의 정보는 기록에 포함되지 않습니다.

- G. 전자 서명(*electronic signature*)은 서명 기록의 의도로 개인이 작성 또는 적용하여 전자기록에 첨부 또는 연합한 전자 소리, 심벌, 절차입니다.
- H. 부적절한 자료(*Inappropriate materials*)는 미성년자/학생에게 해가 되는 외설 또는 포르노 자료로 성인/성욕적 내용에 관련된 웹사이트, 나이에 부적절한 자료, 이 규정에 따라 교육적 목적이 아니거나 교육구의 보안 또는 MCPS 정책과 정책에 따르지 않은 자료를 포함합니다. 부적절한 자료에는 또한, 해킹, 약물, 알코올, 담배의 사용, 배급, 제조, 불링, 희롱, 협박, 범죄기술, 폭력, 총기의 불법적 사용 또는 소지를 육성하거나 조장하는 모든 것을 포함합니다. 실제 연구조사 또는 교직원이 명시하는 법적 목적으로 필요할 경우, 적절한 접근을 허락받을 수도 있습니다.
- I. 인터넷 접속(*Internet access*)은 인터넷 서버와 사용자 간의 연결에 사용되는 모든 승인된 방법과 이를 제공하기 위한 승인된 모든 방법을 포함합니다.
- J. 테크놀로지 보호 측정(*technology protection measure*)은 인터넷 필터링 기술로 특정 항목을 제한할 수 있도록 구성된 인터넷에서 선택한 부분만 제한하도록 또는 부적절한 자료에의 접근을 예방하도록 구성된 기술입니다.
- K. 인가되지 않은 도구/기기(*Unauthorized equipment*)는 Office of the Chief Technology Officer(OCTO)와/또는 대리인이 MCPS 컴퓨터, MCPS 네트워크에의 연결을 승인하지 않은 모든 기기입니다. 이에에는 다음을 포함 그러나 이에 제한되지 않습니다: 컴퓨터, 태블릿 기기, 무선 액세스 포인트, 스마트폰, 휴대전화 등과 같은 개인 커뮤니케이션과 구성용 기기, 사진기기, MP3 플레이어 또는 iPods™와 같은 오락성 기기.
- L. 사용자(*user*)는 모든 MCPS 교직원, 학생, 기타 MCPS 컴퓨터 시스템 사용을 승인받은 개인입니다. 기타 개인에는 학부모, 자원봉사자, 계약자/직원, 임시 직원을 포함할 수 있습니다.

IV. 행정절차

다음 항목 기술 절차는 전자 데이터, 정보 보안, 전가 전환, 서명, 실제 보안 시스템과 앱 보안, 네트워크 보안의 실행과 사용을 위한 사이버 안전, 사이버 보안, 사이버 윤리를 위한 요건입니다. 컴퓨터 시스템 보안담당을 위한 특정 사용자의 책임과 절차는 MCPS 웹사이트 *Manual of MCPS Computer Systems Security Procedures* 에 있습니다.

- A. 전자 데이터와 정보 보안(Electronic data and information Security)

사용자는 본인의 과제/업무와 책임을 위해 필요한 승인된 정보와/또는 컴퓨터 시스템에만 접근할 수 있습니다

1. 사용자는 개인 어카운트에 책임이 있습니다.
 - a) 사용자는 철저한 보안을 위해 패스워드를 변경해야 합니다.
 - b) 사용자의 어카운트와 패스워드 공유는 금지되어 있습니다.
 - c) 개인 어카운트 이름과 연결되어 있는 모든 위반행위는 어카운트 주인의 책임입니다.

2. 사용자는 컴퓨터 앞을 떠날 때나 타인에게 사용하도록 할 때, 모든 시스템에서 로그오프해야 합니다.

3. 이 규정에 따른 보안 절차에 관해 알고 조심하며 이에 따르는 것은 모든 사용자의 책임입니다.

4. 사용자는 전자 데이터를 안전하게 보관해야 합니다. (메모: 중요한 파일은 개인 네트워크 폴더/디렉터리 또는 열쇠로 잠글 수 있는 파일 캐비닛, 서랍 등에 넣을 수 있도록 외장 하드나 USB 메모리 등에 옮겨서 안전한 곳에 보관해야 합니다.)

5. MCPS 는 시스템 불량이나 중지에 따른 정보 상실에 어떠한 책임도 없습니다. 사용자는 백업카피를 만들어 안전한 곳에 보관해야 합니다.

B. 전자 전환과 서명(Electronic Transactions and Signatures)

Maryland 주법, 연방법, MCPS 정책 또는 규정에서 처리에 관한 부여자의 서명을 요구할 경우, 전자기록에 적절한 전자 서명 방법을 통한 전자 서명이 있으면 이를 충족한 것으로 간주합니다. 전자 처리와 서명에 관한 절차와 승인은 *Manual of the MCPS Computer Systems Security Procedures* 에 간략하게 명시되어 있습니다.

C. 물체의 보안(Physical Security)

컴퓨터 시스템 기기를 안전한 환경에 놓고 관리해야 합니다. 사용자는 다음 컴퓨터와 관련 테크놀로지의 안전 보관 수칙에 따를 책임이 있습니다.

1. 교직원이 감독할 수 없을 경우, 귀중한 컴퓨터와 기기를 보관하는 임시 또는 장기 보관 포함한 모든 장소를 안전하게 잠가야 합니다.
2. 컴퓨터와 관련 기기는 적절한 승인 없이 MCPS 소유지를 벗어나서는 안 됩니다.
3. 사용자는 컴퓨터 또는 관련 기기의 장소의 책임 절차에 따른 사인인과 사인아웃 절차를 따라야 합니다. 이 기기는 사용자가 MCPS 를 떠나거나 다른 학교 또는 사무실로 이전할 경우, 학교, 사무실, 부서, 기관에 반납해야 합니다.
4. 지역 기기 재고는 최대한 정확하게 관리되어야 합니다. 기기는 취득할 당시 재고 목록에 추가하게 됩니다. 사용자는 재고 표시나 재고 관리표를 컴퓨터에서 떼지 말아야 합니다.
5. 기기를 분실 또는 도난당한 경우, MCPS Regulation EDC-RA, *Control of Furniture and Equipment Inventory* 에 따라 취급을 하게 됩니다.

D. 시스템과 애플리케이션 보안(Systems and Applications Security)

1. 사용자는 *Manual of MCPS Computer Systems Security Procedures* 에 명시된 바와 같이, 컴퓨터 또는 기타 승인된 디지털/전자 기기에 설치되어 있는 소프트웨어 또는 하드웨어를 적절한 교직원의 승인 없이 어떠한 목적으로도 설치해서는 안 되며, 보안 세팅 또는 보호조치(안티바이러스 소프트웨어 등)을 작동 못하게 또는 조정해서는 안 됩니다.
2. 사용자는 적절한 교직원의 승인 없이 *Manual of MCPS Computer Systems Security Procedures* 에 명시된 바와 같이, 시스템을 변경해서는 안 됩니다.
3. MCPS 소프트웨어와 애플리케이션은 라이선스 동의서에 명시된 경우를 제외하고 MCPS 소유가 아닌 컴퓨터에 설치 또는 복사할 수 없습니다.

E. 네트워크 보안(Network Security)

MCPS 네트워크와 정보로의 모든 접속은 MCPS 가 승인한 권한 담당 OCTO 의 승인이 필요합니다. 이를 어기거나 MCPS 정책 또는 규정의 적용을 위반하여

네트워크 또는 정보에 접근할 경우, 사용자의 어카운트 또는 접속은 삭제, 정지, 무효화될 수 있습니다.

F. 관리와 사용(Conduct and Use)

학생과 교직원의 인터넷 사용은 테크놀로지 또는 직접 감독을 포함 그러나 이에 제한하지 않고 양한 방법을 통해 모니터링하게 됩니다.

1. 이 규정에서 규정한 바와 같이, 사용자는 네트워크에의 접속 또는 네트워크 자료의 유입이 교육적 목적임을 확실히 이해할 의무가 있습니다.
2. 어떠한 자료 또는 정보를 의도적으로 MCPS 시스템 또는 인터넷 사이트에 게재 또는 링크할 경우, 이 규정에 명시한 바와 같이 교육적 목적이어야 합니다.
3. 사용자는 MCPS 기기로서의 인터넷 연결로 사용하게 되는 모든 것을 포함하여, 사용하는 컴퓨터 시스템의 사용 규칙에 따를 의무가 있습니다.
4. MCPS 는 사용자가 MCPS 를 통해 접하는 다른 시스템 또는 인터넷 사이트에 있는 정보를 조정하거나 책임질 수 없습니다. MCPS 외부의 사이트 또는 시스템 중에는 비방, 부정확, 악용, 외설, 저속, 성적, 위협적, 인종차별적 또는 불법 자료가 포함되어 있을 수 있습니다.
5. 모든 컴퓨터 시설, 네트워크, 타 테크놀로지 자원의 사용은 Section III.D.에 명시된 바에 따라, 교육적 목적을 위해서만 사용해야 하며, MCPS 가 검토하고 기록 또는 보관할 수도 있습니다.
6. MCPS 이메일은 교육적 목적으로만 사용됩니다. 모든 실행 내용은 MCPS 의 점검을 받고 기록 및 보관될 수 있습니다. MCPS 이메일을 사용하는 모든 학생은 학습 절차를 돕거나 활성화하기 위한 목적으로만 승인됩니다.
7. 학생의 승인되지 않은 이메일, 인스턴트 메시지, 채팅방 사용은 금지되어 있습니다.
8. 모든 부적절한 행동과 부적절한 컴퓨터 시설 사용을 모두 표기하는 것은 불가능합니다만, 다음 지침은 금지된 컴퓨터와 네트워크의 사용 위반의 예를 제공합니다:

- a) 시스템의 무단 변경(또한, 해킹으로도 알려짐) 또는 방법을 제공하여 타인의 무단 변경을 돕는 행위, MCPS 시스템 (승인되지 않은 대체 행정 시스템, 개인 어카운트, 네트워크 공유폴더, 소프트웨어, 네트워크 시설과/또는 기타 프로그램) 을 무단 변경하는 정보 제공과/또는 시설 파손.
- b) 패스워드의 해독, 키 로깅 또는 하드웨어 기기나 소프트웨어 애플리케이션을 사용한 승인되지 않은 패스워드 캡처 그리고/ 또는 승인되지 않은 상위 수준의 접속, 특권 또는 이를 위한 시도.
- c) 다른 사용자 네트워크 접근 또는 컴퓨터 사용을 서비스 거부 공격(denial of service-DoS)을 통해 고의적으로 훼방하는 행위 또는 분산형 서비스 방해 행위(distributed denial of service-DDoS).
- d) 중상, 명예를 훼손 또는 타인을 사이버불링, 희롱, 협박하는 글이나 행동.
- e) 위의 III. H 에 명시한 바와 같은 부적절한 자료에 고의적으로 접근 또는 접근 시도.
- f) MCPS 컴퓨터 시스템을 해치거나 전복시키려는 의도로 제공되는 바이러스 또는 웜과 같은 악성코드/소프트웨어의 진행.
- g) OCTO 와/또는 OCTO 대리인 없이 MCPS 컴퓨터 또는 MCPS 네트워크에 승인되지 않은 기기의 접속.
- h) 이메일을 사용하여 위협 또는 원하지 않는 벌크 이메일 그리고/또는 인터넷의 상업 메시지를 제공하여 사기적 취득 또는 개인정보 도용, 취득을 위한 사기적 이메일의 사용.
- i) 프록시 서버나 애플리케이션 또는 기타 방법을 사용하여 네트워크 보안 또는 필터링 기술로 알려진 기술보호조치를 피하기.

- j) 다른 사용자의 이메일을 승인 없이 삭제, 위조 또는 읽거나 복사하거나 이와 같은 행동을 시도.
 - k) 다른 사용자의 데이터 파일을 학교 교육감 및/또는 대리인의 승인 없이 읽기, 삭제, 복사, 전송, 프린트, 공유, 개조.
 - l) 개인의 MCPS 이메일, 주소, 어카운트, 패스워드를 타인이 사용하도록 허락하는 행위.
 - m) 개인의 MCPS 네트워크 어카운트, 네트워크 폴더, 패스워드를 타인이 사용하도록 허락하는 행위.
 - n) MCPS 시스템의 상업 광고용, 체인 메일, 비교육적 게임으로의 사용.
 - o) 저작권 자료나 소프트웨어를 승인 없이 복사 또는 전환.
 - p) MCPS 기기 또는 자료를 사용하여 학생 또는 교직원에게 승인되지 않거나 거짓 정보 즉 개인 식별정보를 전자로 게재 또는 유포.
 - q) 개인의 이익 또는 불법 행위를 위해 MCPS 네트워크 또는 컴퓨터 시스템을 사용.
9. 모든 사용자의 미성년자의 개인 정보를 승인 없이 공개, 사용, 유포에의 의도적인 참여를 금지합니다.
 10. 학생은 소셜네트워크 사이트와 채팅방, 사이버불링 예방과 각성 및 대응을 포함한 적절한 온라인 사용에 관한 교육을 받습니다.
 11. 기술보호조치를 통한 필터를 통하지 않은 부적절한 자료를 인터넷에서 발견한 MCPS 컴퓨터 시스템 사용자는 MCPS 웹사이트에 있는 *Manual of MCPS Computer Systems Security Procedures* 에 명시되어 있는 절차를 따라야 하며 또한 따를 것을 기대합니다.

V. 불이행(NONCOMPLIANCE)

- A. 절차와 이 규정 기준에 따르지 않을 경우, 이에 따른 적절한 징계/훈육 조치를 받게 됩니다.

1. 직원의 징계는 회의, 경고, 견책 평지, 혜택의 박탈, 무급 휴직, 견책, 해고와/또는 범죄 기소입니다.
2. 학생의 징계/훈육 조치는 부모/후견인과의 전화, 혜택을 잃거나, 손해 배상, 정학과/또는 퇴학 그리고/또는 범죄 기소를 포함 그러나 이에 제한하지 않습니다. (MCPS Regulation JFA-RA, *Student Rights and Responsibilities*,와 학교 훈계 정책 참조)
3. 타 사용자에의 징계/훈계 조치는 혜택의 박탈과/또는 범죄 기소입니다.

B. MCPS 컴퓨터 시스템 사용자는 의심되거나 적절하지 않은 데이터 사용, 컴퓨터 시스템 남용 또는 보안 위반 가능성을 신고해야 합니다. 학교를 기반으로 하는 사용자는 학교장 또는 정보 테크놀로지에 관해 책임이 있는 학교장 대리인에게 알려야 합니다. 학교 외 기반 사용자는 즉시 스퍼바이저와 교육감 또는 대리인에게 즉시 알려야 합니다. *Manual of MCPS Computer Systems Security Procedures* 에 명시된 심각한 위반이나 침해는 또한 OCTO 에게 보고해야 합니다.

규정 변경사: 1995년 8월 22일 새 규정; 1999년 12월 13일 갱신; 2000년 6월 1일 사무실 이름 갱신; 2002년 6월 10일 갱신, 2007년 5월 23일 갱신; 2012년 7월 27일 갱신.