

허용가능한 인터넷 사용 및 보안 정책
2001 년 2 월 14 일 교육청 결의안 실행
2012 년 7 월 1 일 개정

허용가능한 인터넷 사용 및 보안 정책(IAUSP)

정책

뉴욕시 교육청 ("교육청")에서는 집합적으로 "사용자"라고 일컬어지는 직원, 에이전트, 학생, 자원봉사자들에게 교육 및 업무 수행을 위해, 적용되는 법률에 부합하여 교육청의 인터넷 시스템에 접속할 수 있도록 허용하고 있습니다. 허용가능한 인터넷 사용 및 보안 정책 ("정책")은 교육청 이메일 및 교육청 제공 인터넷 접속을 포함한 교육청의 인터넷 사용 및 접속에 관한 모든 사용자의 컴퓨터 사용관련 활동을 관장하며 교육청 소유 기기를 이용하거나 기타 기기를 이용하는 모든 경우의 교육청 인터넷 시스템의 사용에도 적용됩니다.

"교육청의 인터넷 시스템"은 교육청 제공, 기기, 교육청에서 제공하는 인터넷 연결 (무선 연결 시스템 포함), 교육청 제공 이메일 계정, 인트라넷 및 기타 교육청 시스템의 원거리 접속 등을 의미합니다. 사용자의 물리적 위치에 관계 없이 어떤 기기 (해당 기기가 교육청에서 제공한 기기인지의 여부에 관계 없이)를 이용하여 교육청의 인터넷 시스템을 통해 실행한 모든 컴퓨터 상에서 이루어진 활동은 사용자가 교육청의 인터넷 시스템에 접속 및 이용을 한 것으로 간주됩니다.

"교육청 제공 기기"는 데스크톱 컴퓨터, 랩톱 및 PDA, 스마트폰, 아이패드, 테이블릿 및 이-리더와 같은 휴대용 단말기만에 국한되지 않고 이를 포함한 교육청에서 제공한 모든 전자 기기를 의미합니다.

교육청의 인터넷 시스템을 이용하는 학생은 이 정책, 교육청 규정, 정책 및 가이드라인, [뉴욕시 품행 표준 및 동일한 징계 방법](#) ("규율 규정") 및 적용가능한 법률에 따라 관리받습니다. 직원의 사용은 이 정책, 교육청 규정, 정책과 가이드라인, 교육청의 고용 정책, 적용가능한 총괄 교섭 협약과 적용가능한 법률에 따라 관리됩니다.

교육청의 인터넷 시스템을 이용함으로써, 사용자는 이런 정책, 모든 적용가능한 교육청 규정, 정책과 가이드라인을 준수할 것에 동의합니다. 모든 사용자들은 반드시 네트워크 또는 인터넷의 오용이나 이 정책을 위반한 모든 커뮤니케이션의 교환에 대해 교사, 수퍼바이저 또는 기타 적절한 교육청 직원에게 보고하여야 합니다.

허용가능하고 안전한 인터넷 이용의 원칙

일반적인 원칙

교육청에서 제공한 인터넷의 접속과 이메일의 사용은 교육적 사용, 지도, 리서치 및 커뮤니케이션 지원, 협력과 기타 교육청 관련 목적을 위해서 사용되어야 합니다. 사용자들은 교실 및/또는 일반적인 업무 장소에서 기대되는 것과 동일한 기준의 적용을 받습니다.

감독 및 프라이버시

교육청의 인터넷 시스템을 사용할 때, 사용자는 프라이버시를 가질 수 없습니다. 교육청은 사용자의 온라인 활동을 감독하고 모든 전자 커뮤니케이션이나 파일에 대한 접속, 검토, 복사, 저장 및 삭제할 권리를 갖습니다. 여기에는 교육청 제공 기기에 저장된 파일, 이메일, 쿠키 및 인터넷 사용 내역을 포함한 모든 아이템이 포함됩니다.

교육청은 법 집행 담당자 또는 제 삼자가 적절하고 적용가능한 법률에 따라 요구한 전자 커뮤니케이션을 포함한 모든 컴퓨터 이용 활동을 공개할 권리를 갖습니다. 교육청은 교육청 인터넷 시스템을 통해 이루어진 모든 불법적인 활동에 대한 우려나 관련에 대한 로컬, 주 또는 연방 기관들의 모든 법적인 조사에 전적으로 협력할 것입니다.

교육청 인터넷 시스템의 금지된 사용

사용자들은 교육청의 인터넷 시스템을 이용할 때 이 정책이 금지한 어떤 활동에도 참여하지 않도록 합니다.

사용자가 어떤 활동이 금지된 활동인지 확실하지 않다면, 교사, 수퍼바이저 또는 기타 적절한 교육청 직원에게 문의하여야 합니다. 교육청은 (1) 교육청, 학생, 직원, 학교, 네트워크 또는 컴퓨터 리소스에 대한 보안 및/또는 안전 문제를 일으키거나, 또는 (2) 교육청에서 교육적 또는 교육청 내용이나 목적에 적절하지 않다고 결정한 내용에 교육청 리소스를 확대하거나 또는 (3) 교육청이 부적절하다고 판단한 경우에 이런 활동에 대한 즉각적인 조치를 취할 수 있는 권리를 갖습니다.

다음은 금지된 행동의 비-포괄적인 목록의 예입니다:

1. 타인에게 해를 끼치거나 다음과 같이 타인이나 교육청의 소유물을 파손시킨 경우:
 - a. 욕설, 음란한 말, 저속한 말, 헐박 또는 폭력적인 언어 등을 이메일 메시지, 교육청 웹 페이지 게시 또는 전문적인 소셜 미디어 사이트에 게시, 또는 배포;
 - b. 포르노 같거나 외설스럽거나, 불법적이거나 위험한 행동을 부추기거나 또는 폭력이나 차별을 주장하는 정보나 자료를 접속, 이용, 게시 또는 배포; 만약 사용자가 이런 정보에 의도하지 않고 접속하였다면, 이런 의도하지 않았던 접속에 대한 상세한 내용을 본인의 소속 학교 또는 중앙 부처에 즉시 보고하여야 합니다.
 - c. 괴롭히고, 차별하고, 자극적이고 미움을 조장하는 자료나 다른 사람에 대한 피해를 조장하거나 거짓을 접속, 게시 또는 배포;
 - d. 체인메일 또는 스팸 메일을 전송, 게시 또는 배포;
 - e. 컴퓨터 바이러스 전염, 데이터, 소프트웨어나 부속품 훼손, 또는 기타 전자기기를 고장내거나 교육청의 교육이나 업무 환경의 중단을 초래할 원인이 될 수 있는 행동에 참여하는 것을 포함한 컴퓨터 기기, 파일, 데이터 또는 교육청의 인터넷 시스템을 파손시키는 모든 행동;
 - f. 사용자의 교육적 목적 또는 사용자의 업무 능력이 저해되도록 교육청의 인터넷 시스템을 사용;
 - g. 적용되는 지적 재산 보호법을 위반한 음악, 사진, 비디오 또는 기타 내용을 다운로드, 게시, 재생산 또는 배포; 모든 음악, 사진 및/또는 비디오는 교육청을 위해서만 다운로드 받아야 하며 개인적인 목적으로 이용해서는 않습니다. 만약 어떤 자료의 활용 방법이 상술되어 있다면, 해당 사용자는 이렇게 명시된 요건을 따라야 합니다. 만약 사용자가 어떤 자료를 사용할 수 있을지 여부를 확실히 알 수 없다면, 저작권이나 상표 소유주에게 사용 허가를 요청하거나; 또는
 - h. 표절을 하게 될 것입니다. 표절은 타인의 아이디어나 글을 도용하여 사용자 본인의 독창적인 아이디어로 제출하는 것입니다.

2. 교육청 인터넷 시스템, 또는 어떤 제 삼의 컴퓨터 시스템에 다음과 같이 허용되지 않은 접속을 하거나 접속을 하고자 시도하는 경우:
 - a. 고의적인 변경, 피싱 또는 해킹 행위;
 - b. 다른 사용자의 비밀번호를 의도적으로 알아내려고 시도;
 - c. 다른 개인에게 교육청 인터넷 시스템 상의 기타 사용자 비밀번호를 공개; 그러나, 학생들은 학부모님들과 본인의 교육청 비밀번호를 공유할 수도 있습니다.
 - d. 다른 사용자의 비밀번호 변경;
 - e. 타인의 계정으로 로그인하려고 시도;
 - f. 교육청에서 막아 놓았거나 필터링한 자료에 접속하려고 시도;
 - g. 다른 사용자의 파일을 허가 없이 접속, 복사 또는 수정;
 - h. 사용자의 신분을 속인 경우;
 - i. 사용자 본인의 것이 아닌 계정의 비밀번호나 아이디를 이용; 또는

j. 다른 사람이 계정 또는 기타 컴퓨터 네트워크에 접속하는 것을 위협하는 행위를 한 경우.

3. 교육청의 인터넷 시스템을 다음과 같은 상업적인 목적으로 사용한 경우:

- a. 교육청의 인터넷 시스템을 본인의 금전적 이익을 위해 사용;
- b. 수익을 창출하는 사업 활동, 개인적인 선전 또는 기타 비-교육청 업무를 위한 커뮤니케이션;
- c. 기금 모금 활동 (교육감 규정 A-610 에 정해진 내용 외); 또는
- d. 교육청의 인터넷 시스템에 선출 공무원, 후보, 후보들, 후보 명단 또는 정치적인 조직 또는 위원회를 위해 사용한 경우.

4. 범법 또는 기타 불법적인 활동에 참여.

필터링

아동의 인터넷 보안법 (Children's Internet Protection Act: "CIPA")에 따라, 교육청은 교육청에서 미성년자에게 부적절하다고 판단한 인터넷 상의 내용을 금지하거나 필터링합니다. 여기에는 포르노, 외설적인 자료 및 기타 미성년자에게 해로운 내용이 포함됩니다. 교육청은 부적절하다고 여겨지는 기타 내용, 교육적 또는 업무 관련도가 부족한 내용 또는 네트워크에 위해를 가할 수 있는 내용을 금지하거나 필터링할 수도 있습니다. 교육청은 자체적 판단에 따라, 선의의 리서치 또는 기타 법률적인 교육 또는 업무 목적으로 일부 사용자들에게 이런 필터링을 해제시켜줄 수도 있습니다.

사용자들은 네트워크의 필터링을 해제할 수 있는 어떤 웹사이트, 어플리케이션 또는 방법을 이용하거나 기타 어떤 불법적인 활동도 수행해서는 안될 것입니다.

CIPA 에 관한 추가적인 정보를 원하시면 아래 링크를 참조하십시오:

<http://www.fcc.gov/guides/childrens-internet-protection-act>

개인 신분을 판별할 수 있는 비밀 정보 보호

가정의 교육 권리와 사생활보호 법(Family Educational Rights and Privacy Act: "FERPA")은 교육청 학교 직원들이 교육청의 교육관련 기록으로부터 학생들과 가정의 **개인 신분을 판별할 수 있는 정보** (personally identifiable information: "PII")를 학부모 동의 없이 제 삼의 기관에 공개하는 것을 불허하고 있습니다. 그러나 이런 일반적인 규칙에 몇 가지 예외가 적용됩니다.

교육청의 인터넷 시스템의 모든 사용자들은 반드시 FERPA 및 [교육감 규정 A-820](#), 비밀보장과 학생 기록 공개; 기록 유지를 준수하여야 합니다. 만약 귀하의 활동이 FERPA 또는 교육감 규정 A-820 에 부합하는지 여부가 확실하지 않다면, 교육청의 정보 보안 총괄 (Chief Information Security Officer)에게 연락하십시오.

교육청 변호사들과의 내부 커뮤니케이션 또한 비밀입니다. 따라서, 사용자들은 변호사와 먼저 확인하지 않고도 이런 커뮤니케이션을 전달하거나 배포하지 않도록 해야합니다. 사용자들은 기밀 정보가 포함되었거나 첨부된 이메일들이 관련 정보가 전달되어야만 하는 사람들에게만 전달될 수 있도록 조심하여야 합니다.

학생 인터넷 안전

1. 교육청 책임:

- a. 교육청은 소셜네트워크 웹 사이트, 채팅룸에서 타인과 접촉하기 및 인터넷 왕 따에 대한 인식과 대응을 포함한 적절한 온라인 행동에 관한 커리큘럼을 제공할 것입니다.

- b. 교육청은 미성년자들이 이메일, 채팅룸 및 기타 직접적인 전자 커뮤니케이션에 참여할 때, 이들의 안전과 보안을 유지할 수 있도록 노력할 것입니다.
- c. 적절하다면, 교육청은 인터넷을 사용하는 동안 학생 안전에 대한 가이드라인과 지침을 학생, 직원 및 학부모에게 제공할 것입니다.

2. 학생들의 교육청 인터넷 시스템 사용

- a. 학생들은 소셜네트워킹 사이트, 채팅룸, 이메일 또는 기타 직접적인 전자 커뮤니케이션이나 기타 모든 형태의 인터넷 사용에 있어 본인이나 타인에 대한 개인적인 정보를 절대로 밝혀서는 안될 것입니다. 예를 들어, 학생들은 절대로 본인의 집 주소, 전화번호 또는 핸드폰 번호를 알려서는 안될 것입니다. 학생들은 절대로 본인의 사진이나 타인의 사진을 게시해서는 안될 것입니다.
- b. 학생들은 인터넷 상에서만 접촉했던 어떤 사람도 만나지 않도록 합니다.
- c. 학생들은 부적절하거나 불편한 감정을 갖게하는 어떤 정보를 받았다면 반드시 본인의 교사 또는 기타 학교 직원에게 즉시 알려야 합니다.
- d. 학생들의 비밀번호를 교육청 컴퓨터에 저장하는 것이 허용되지 않아야 할 것입니다.

3. 수업 활동을 위해 소셜 미디어를 포함한 교육청 인터넷 시스템을 사용하는 교사

- a. 교사들은 소셜네트워킹 웹사이트, 채팅룸에서 타인과 접촉하기 및 인터넷 왕 때에 대한 인식과 대응을 포함한 안전한 온라인 이용에 대한 교육을 할 것입니다. 교사들은 [디지털 시대의 교육청 시티즌십 안내](#), 및 온라인에서 구할 수 있는 기타 무료 교육적인 인터넷 안전 리소스를 참고하도록 합니다.
- b. 소셜 미디어
 - "소셜 미디어"는 소셜 네트워크, 블로그, 인터넷 웹사이트, 인터넷 포럼 및 위키만이 아니라 이를 포함한 쌍방향 커뮤니케이션을 허용하는 모든 형태의 온라인 발행물이나 존재를 의미합니다. 소셜 미디어에는 페이스북, 트위터, 유튜브, 구글 플러스 및 플리커 등이 있습니다.
 - 학교에서는 학생들의 교육과 학습을 강화하기 위한 다양한 온라인 기반의 쌍방향 커뮤니케이션 기술을 이용하고 있습니다. 소셜 미디어 사이트는 반드시 수업 및 과제와 연결되어 교사와 기타 학생들 사이의 커뮤니케이션을 지원하기 위한 교육 및 학교 관련 목적으로만 사용되어야 합니다.
 - 교육청은 교육청 및 교육청 소속 학교 직원들 사이에 개별적으로 이들 사이트에 접속하는 것을 제한하고 있습니다. 만약 소셜미디어 사이트의 접속에 교육청 또는 교육청 소속 학교 직원들이 아닌 사람들까지 포함된다면, 학부모 동의가 필요합니다.
 - 만약 인터넷 사용에 소셜미디어가 포함된다면, 교사들은 반드시 교육청의 이 정책과 접목된 [소셜미디어 가이드라인](#)을 참고하여야 합니다.

4. 학부모:

- a. 일반적으로 학생들이 학교 건물에서 교육청의 인터넷 시스템을 이용할 때는 감독을 받게 되지만, 학생들이 인터넷을 사용할 때 마다, 교육청에서 다양한 사회적 가치를 관리하고 준수하도록 지키는 것이 현실적이지 않습니다. 학부모님들께서는 자녀들에게 특정한 가족 가치관에 대한 전달에 관한 일차적인

책임을 갖고 있으며 어떤 자료가 교육청 인터넷 시스템을 통해 자녀분이 접속을 해도 될 지의 여부에 관해 대화를 나누시기 바랍니다.

- b. 학부모님들은 자녀분이 가정이나 학교가 아닌 장소에서 교육청의 인터넷 시스템에 접속할 때, 자녀분의 인터넷 사용에 대한 감독을 하셔야 할 전적인 책임을 갖습니다. 교육청은 가정의 교육청 인터넷 시스템 접속을 필터링 하거나 그렇지 않을 수도 있습니다. 학부모님들께서 학교나 교육청에 문의하시기 바랍니다.

이 정책의 위반

중앙 부처와 학교를 포함한 교육청은 교육청 이메일을 포함한 교육청 인터넷 시스템에 대한 어떤 사용자의 접속 여부도 언제든지 종료할 수 있는 권리를 갖고 있습니다.

만약 학생이 이 정책을 위반하였다면, 규율 규정 및 관련 교육감 규정에 부합한 적절한 징계 조치가 취해질 것입니다. 만약 학생의 교육청 인터넷 시스템 접속 권리가 취소되었다면, 해당 학생은 학업적인 면으로 불이익을 받지 않을 수 있으며 교육청은 교육 프로그램에 참여할 수 있는 의미있는 기회를 지속적으로 해당 학생에게 제공할 것입니다.

직원 이 이 정책을 위반하였다면 적절한 징계 절차에 따라 처리될 것입니다.

모든 사용자들은 부적절하거나 불편한 감정을 갖게하는 어떤 정보를 받았다면 반드시 본인의 교사, 슈퍼바이저, 교장 또는 관리자에게 즉시 알려야 합니다.

책임 제한

교육청은 제공된 서비스의 품질에 대한 보장을 할 수 없으며 네트워크 또는 계정의 사용으로 발행할 수 있는 어떤 손실, 손해, 훼손, 비용 또는 기타 책임에 대한 책임을 갖지 않습니다. 교육청 네트워크를 사용하여 사용자가 축적한 어떤 추가적인 비용도 사용자가 책임을 갖습니다. 교육청은 또한 사용자가 접속하여 찾은 정보의 정확성이나 수준에 대한 어떤 책임도 부정합니다. 컴퓨터 네트워크 또는 인터넷으로 접속한 어떤 문건도 교육청, 교육청 관련 기관 또는 직원의 것이 아닌 작성자 개인의 개별적인 관점으로 인식되어야 합니다.

이 정책의 사본과 문의

교육청은 필요가 발생한다면 언제든지 이 정책의 수정 및/또는 개정을 할 수 있는 권리를 갖습니다. 이 정책의 사본은 요청에 따라 제공될 수 있으며 다음의 교육청의 웹사이트에서 구하실 수도 있을 것입니다:

<http://schools.nyc.gov/Offices/EnterpriseOperations/DIIT/WebServices/iaup/default.htm#preamble>.

본 규정에 대한 문의는 아래 연락처로 하십시오:

NYC Department of Education
Office of Communications & Media Relations
52 Chambers Street, Room 314
New York, NY 10007
전화: 212-374-5141
팩스: 212-374-5584