York Adams Academy
Title: Acceptable Use of Computers, E-mail, Network Resources, and Internet Access
Number: 815
Status: Active

Legal

17 U.S.C. 101 et seq
18 U.S.C. 2256
20 U.S.C. 6777
47 U.S.C. 254
18 Pa. C.S.A. 5903
18 Pa. C.S.A. 6312
24 P.S. 1303.1-A
24 P.S. 4604
24 P.S. 4610
24 P.S. 4601 et seq
47 CFR 54.520
Pol. 103
Pol. 103.1
Pol. 104
Pol. 317
Pol. 814

Purpose

The Joint Board of Directors ("Board") of the York Adams Academy ("Academy") supports the use of the computers, Internet and other network resources in the Academy's instructional and operational programs in order to facilitate learning, teaching and daily operations through interpersonal communications and access to information, research and collaboration.

Internet access, electronic mail (e-mail) and computers and network resources shall be made available to teachers, administrators, support staff, students and other authorized individuals ("users") for educational and instructional purposes and other purposes consistent with the educational mission of the Academy, as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.

The purpose of this policy is to outline expectations for acceptable and responsible use of Academy technology resources by students, staff and the community ("all users"). For purposes of this policy, the term, "technology resource" includes but is not limited to any Academy-owned, leased or licensed or user-owned personal hardware, software, or other technology, including cell phones and personal electronic devices, used on Academy premises or at Academy

events. Access to Academy technology and network resources is a privilege, not a right. All users will be held accountable for noncompliance with this policy.

Definitions

The term "child pornography" is defined under both federal and state law.

Child pornography - under federal law, is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

1. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

2. Such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or

3. Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

Child pornography - under state law, is any book, magazine, pamphlet, slide, photograph, film, videotape, computer depiction or other material depicting a child under the age of eighteen (18) years engaging in a prohibited sexual act or in the simulation of such act.

The term "harmful to minors" is defined under both federal and state law.

Harmful to minors - under federal law, is any picture, image, graphic image file or other visual depiction that:

1. Taken as a whole, with respect to minors, appeals to a prurient interest in nudity, sex or excretion;

2. Depicts, describes or represents in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or lewd exhibition of the genitals; and

3. Taken as a whole lacks serious literary, artistic, political or scientific value as to minors.

Harmful to minors - under state law, is any description or representation in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it:

1. Predominantly appeals to the prurient, shameful, or morbid interest of minors;

2. Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable for minors; and

3. Taken as a whole lacks serious literary, artistic, political, educational or scientific value for minors.

Obscene - any material or performance, if:

1. The average person applying contemporary community standards would find that the subject matter taken as a whole appeals to the prurient interest;

2. The subject matter depicts or describes in a patently offensive way, sexual conduct described in the law to be obscene; and

3. The subject matter, taken as a whole, lacks serious literary, artistic, political, educational or scientific value.

Technology protection measure - a specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography, or harmful to minors.

Authority

The Academy makes no warranties of any kind, whether expressed or implied, for the service it is providing. The Academy is not responsible, and shall not be responsible, for any information that may be lost, damaged or unavailable when using the network, including loss of data resulting from delays, non-deliveries, missed deliveries, or service interruption. Use of any information obtained through the use of the Academy's computers is at the user's risk. The Academy shall not be responsible for the accuracy or quality of information obtained through the Internet or e-mail. The electronic information available to users does not imply endorsement by the Academy of the content received or displayed.

The Academy assumes no responsibility or liability for any charges incurred by a user. Under normal operating procedures, there will be no cost incurred.

The Board declares that use of the internet, e-mail and network resources is a privilege, not a right. The Academy's computer and network resources are the property of the Academy. The Academy reserves the right to log, monitor, and review Internet, e-mail and other network use without cause and without notice; monitor fileserver space utilization by Academy users; or deny access to prevent unauthorized, inappropriate or illegal activity and may revoke access privileges and/or administer appropriate disciplinary action. Users shall have no right or expectation of confidentiality or privacy with respect to anything they create, store, send, delete, receive or display on or over the Academy's Internet, computers or network resources, including personal files or any use of the Academy's Internet, computers or network resources. The Academy shall cooperate to the extent legally required with the Internet Service Provider (ISP), local, state and federal officials in any investigation concerning or related to any illegal activities conducted through the Academy's Internet, computers and network resources.

Network administrators may review student and staff files and communications to maintain system integrity and ensure that students and staff are using the system only for appropriate purposes. Users should expect that files stored on Academy servers or computers will not be private. The Academy maintains archives of all e-mail messages.

The Board requires all users to fully comply with this policy and to immediately report any violations or suspicious activities to the Superintendent of Record or designee.

The Board establishes the following materials, in addition to those stated in law and defined in this policy, as inappropriate for access by minors:

1. Defamatory.

2. Lewd, vulgar, or profane.

3. Threatening.

4. Harassing or discriminatory.

5. Bullying.

6. Terroristic.

The Academy reserves the right to restrict access to any Internet sites or functions it deems inappropriate through established Board policy, or the use of software and/or online server blocking. Specifically, the Academy employs the use of an Internet filter as a technology protection measure that blocks or filters access to inappropriate matter by minors on its computers used and accessible to adults and students. The technology protection measure shall be enforced during use of computers with Internet access. The Academy shall use a reliable firewall network device for filtering. The Academy cannot guarantee that filters, firewalls and other technology protection measures will be one hundred percent effective.

Upon request by students or staff, the Superintendent of Record or designee shall expedite a review and may authorize the disabling of Internet blocking/filtering software to enable access to material that is blocked through technology protection measures but is not prohibited by this policy.

Upon request by students or staff, the network administrator or designee may authorize the temporary disabling of Internet blocking/filtering software to enable access for bona fide research or for other lawful purposes. Written permission from the parent/guardian is required prior to disabling Internet blocking/filtering software for a student's use. If a request for temporary disabling of Internet blocking/filtering software is denied, the requesting student or staff member may appeal the denial to the Superintendent of Record or designee for expedited review.

Delegation of Responsibility

The Academy shall inform staff, students, parents/guardians and other users about this policy through employee and student handbooks, posting on the Academy web site, and by other appropriate methods. A copy of this policy shall be provided to parents/guardians, upon written request.

All students, employees, parents/guardians and others who use the Internet, e-mail or other network resources must agree to and abide by all conditions of this policy. Each user must sign the Academy's Acceptable Use of Computers and Network form, acknowledging awareness of the provisions of this policy, and awareness that the Academy uses monitoring systems to monitor and detect inappropriate use and tracking systems to track and recover lost or stolen equipment.

In the case of a student, the form will be signed upon admission to the Academy and again upon varying intervals at the discretion of the Superintendent of record or designee. The student's parent(s)/guardian(s) must sign at initial registration. The acknowledgment and consent form will remain valid from year to year.

Administrators, teachers and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discern among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use the information to meet their educational goals.

Students, staff and other authorized individuals have the responsibility to respect and protect the rights of every other user in the Academy and on the Internet.

The Superintendent of Record or designee shall make initial determinations of whether inappropriate use has occurred with consultation of the network administrator as necessary.

The Superintendent of Record or designee shall be responsible for recommending technology and developing procedures used to determine whether the Academy's computers are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedures shall include but not be limited to:

1. Utilizing a technology protection measure that blocks or filters Internet access for minors and adults to certain visual depictions that are obscene, child pornography, harmful to minors with respect to use by minors, or determined inappropriate for use by minors by the Board.

2. Maintaining and securing a usage log.

3. Monitoring online activities of minors.

The Superintendent of Record or designee shall develop and implement administrative regulations that ensure students are educated on network etiquette and other appropriate online behavior, including:

1. Interaction with other individuals on social networking web sites and in chat rooms.

2. Cyberbullying awareness and response.

Guidelines

Network accounts shall be used only by the authorized owner of the account for its approved purpose. Network users shall respect the privacy of other users on the system.

Safety

It is the Academy's goal to protect users of the network from harassment and unwanted or unsolicited electronic communications. Any network user who receives threatening or unwelcome electronic communications or inadvertently visits or accesses an inappropriate site shall report such immediately to a teacher or administrator. Network users shall not reveal personal information to other users on the network, including chat rooms, e-mail, social networking web sites, etc.

Internet safety measures shall effectively address the following:

1. Control of access by minors to inappropriate matter on the Internet and World Wide Web.

2. Safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications.

3. Prevention of unauthorized online access by minors, including "hacking" and other unlawful activities.

4. Unauthorized disclosure, use, and dissemination of personal information regarding minors.

5. Restriction of minors' access to materials harmful to them.

All student demographic information must be stored on Academy-approved servers.

Prohibitions

Users are expected to act in a responsible, ethical and legal manner in accordance with Academy policy, accepted rules of network etiquette, and federal and state law. With respect to all users, the following uses are expressly prohibited:

1. Use for inappropriate or illegal purposes.

2. Use in an illegal manner or to facilitate illegal activity.

3. Use for commercial, private advertisement, for-profit purposes or gambling.

4. Use for lobbying or political purposes.

5. Use for nonwork or nonschool related work.

6. Bullying/Cyberbullying.

7. Use to transmit material likely to be offensive or objectionable to recipients.

8. The unauthorized disclosure, use, or dissemination of personal information regarding minors.

9. Use to upload, create, or attempt to create a computer virus.

10. Use to infiltrate or interfere with a computer system and/or damage the data, files, operations, software, or hardware components of a computer system.

11. The illegal installation, distribution, duplication, reproduction or use of copyrighted software and other copyrighted material.

12. Use to obtain, copy, or modify files, passwords, data or information belonging to other users.

13. Loading or using unauthorized games, programs, files, music, or other electronic media.

14. Use which involves any copyright violation or copying, downloading, or distributing of copyrighted material without the owner's permission, unless permitted in accordance with the fair use guidelines.

15. Hate mail, harassment, discriminatory remarks, threatening statements and other antisocial or inflammatory communications on the network.

16. Use to misrepresent other users on the network.

17. Use of another person's e-mail address, user account, or password.

18. Use to disrupt the work of other persons (the hardware or software of other persons shall not be destroyed, modified, or abused in any way).

19. Use for purposes of accessing, sending, creating, or posting materials or communications that are damaging to another's reputation, abusive, obscene, sexually oriented,

threatening, contrary to Academy policy on harassment, harassing, or illegal.

20. Use to invade the privacy of other persons.

21. Posting anonymous messages.

22. Use to read, delete, copy or modify the e-mail or files of other users or deliberately interfering with the ability of other users to send or receive e-mail.

23. Use while access privileges are suspended or revoked.

24. Any attempt to circumvent or disable the Internet blocking/filtering software without authorization.

25. Use inconsistent with network etiquette and other generally accepted etiquette.

26. Accessing, sending, receiving, transferring, viewing, sharing or downloading obscene, pornographic, lewd, or otherwise illegal materials, images or photographs.

27. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with Board policy.

28. Inappropriate language or profanity.

29. Accessing the Internet, Academy computers or other network resources without authorization.

30. Accessing, sending, receiving, transferring, viewing, sharing or downloading confidential information without authorization.

31. Use which causes or is predicted to cause a substantial disruption to the Academy environment.

Students shall also not:

1. Disclose, use, or disseminate any personal identification information of themselves or other students.

2. Engage in or access chat rooms or instant messaging without the permission and direct supervision of a teacher or administrator.

Student users may not download or install any commercial software, shareware, or freeware onto computers, network drives or disks with the exception of portable storage devices, which may be used with staff or faculty permission.

Personal computing hardware may not be used on the Academy's network.

Security

System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or Academy files. To protect the integrity of the system, these guidelines shall be followed:

1. Employees and students shall not reveal their passwords to another individual.

2. Users are not to use a computer that has been logged in under another student's or employee's name.

3. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.

Users identifying a security problem on the Academy's system must immediately notify the appropriate teacher, coordinator or administrator. Users should not demonstrate a security problem to another user.

Copyright

The illegal use of copyrighted materials is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines and applicable laws and regulations.

Academy Web Site

The Academy shall establish and maintain a web site and shall develop and modify its web pages to present information about the Academy under the direction of the Superintendent of Record or designee. All users publishing content on the Academy web site shall comply with this and other applicable Academy policies.

Users shall not copy or download information from the Academy web site and disseminate such information on unauthorized web pages without authorization from the Superintendent of Record or designee.

Consequences For Inappropriate Use

The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.

The network user shall be responsible for expenses incurred as a result of improper use.

Illegal activities or use of the network; intentional deletion or damage to files or data belonging to others; copyright violations; and theft of services shall be reported to the appropriate legal authorities for possible prosecution.

General rules for behavior and communications apply when using the Internet, in addition to the stipulations of this policy.

Students shall act responsibly, as detailed in the Code of Student Conduct.

Vandalism shall result in loss of access privileges, disciplinary action, and/or legal proceedings. **Vandalism** is defined as any malicious attempt to harm or destroy equipment or data of another user, Internet or other networks; this includes but is not limited to uploading or creating computer viruses.

Failure to comply with this policy or inappropriate use of the Internet, Academy network or computers shall result in usage restrictions, loss of access privileges, disciplinary action, including but not limited to suspensions, expulsions and/or termination of employment, and/or legal proceedings.