Internet Safety Policy

Introduction

Peaster Independent School District is pleased to make available to students and employees (network users) access to interconnected computer systems within the District and to the Internet which provides various means of accessing educational materials and opportunities.

It is stated this is a privilege, and not a right. This policy is intended to be read together with the District's Acceptable Use Policy (AUP). All limitations and penalties set forth in the AUP are deemed to be incorporated into this policy.

The Internet safety policy includes the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are (1) obscene; (2) child pornography; or (3) harmful to minors. This Internet safety policy includes the monitoring of online activities of minors, and the district enforces the operation of such technology protection measures during any use of such computers by minors.

It is the intent of this policy to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity ("hacking"); (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act (CIPA) [Pub. L. No. 106-554 and 47 USC 254(h)].

Technology Protection Measures

To the extent practical, steps shall be taken to promote the safety and security of network users of Peaster Independent School District's online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications even to the exclusion of such sites.

To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet access to inappropriate information, to promote the safety and security of its network users. Specifically, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.

Supervision and Monitoring

It shall be the responsibility of all members of Peaster Independent School District's staff to educate, supervise, and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet Protection Act (CIPA), Neighborhood Children's Internet Protection Act (N-CIPA), and Protecting Children in the 21st Century Act.

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the district's superintendent, superintendent designee, or district technology director.

CIPA Definition of Terms

Key terms are as defined in the Children's Internet Protection Act:

A. Computer-- The term computer includes any hardware, software, or other technology attached or connected to, installed in, or otherwise used in connection with a computer.

B. Access To Internet-- A computer shall be considered to have access to the Internet if such computer is equipped with a modem or is connected to a computer network which has access to the Internet.

C. Technology Protection Measure -- The term technology protection measure means a specific technology that blocks or filters Internet access to visual depictions that are: (1) obscene, as that term is defined in section 1460 of title 18, United States Code; (2) child pornography, as that term is defined in section 2256 of title 18, United States Code; or (3) Harmful to minors.

D. Minor -- The term minor means an individual who has not attained the age of 17.

E. Child Pornography -- The term child pornography has the meaning given such term in section 2256 of title 18, United States Code.

F. Harmful To Minors -- The term harmful to minors means any picture, image, graphic image file, or other visual depiction that (1) taken as a whole and 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 a lewd exhibition of the genitals; and (3) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

G. Obscene -- The term obscene has the meaning given such term in section 1460 of title 18, United States Code.

H. Sexual Act; Sexual Contact -- The terms sexual act and sexual contact have the meanings given such terms in section 2246 of title 18, United States Code.

Adoption

Following normal public notice, this Internet Safety Policy will be adopted by the Peaster School Board at its regular monthly board meeting on November 17, 2011.

The district will continue to evaluate whether or not currently available technology protection measures, including commercial Internet blocking and filtering software, adequately addresses the needs of the school district and will certify its compliance with the Children's Internet Protection Act (CIPA) [Pub. L. No. 106-554 and 47 USC 254(h)].

Individual Responsibility of Parents and Users

All network users and the student's parents/guardians are advised that access to the electronic network may include the potential for access to materials inappropriate for school-aged pupils. Every user must take responsibility for his or her use of the computer network and Internet and stay away from these sites. Parents of minors are the best guide to materials to avoid.

If a computer user finds that other users are visiting offensive or harmful sites, he or she should report such use to the campus administrator and/or technology director.

Personal Safety

Be safe. In using the computer network and Internet, do not reveal personal information such as your home address or telephone number. Do not use your real last name or any other information which might allow a person to locate you without first obtaining the permission of a supervising teacher. Do not arrange a face-to-face meeting with someone you "meet" on the computer network or Internet without your parent's permission (if you are under 18). Regardless of your age, you should never agree to meet a person you have only communicated with on the Internet in a secluded place or in a private setting.

Cyber-bullying

"Cyberbullying is when a child, preteen or teen is tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another child, preteen or teen using the Internet, interactive and digital technologies or mobile phones. It has to have a minor involved on both sides, or at least have been instigated by a minor against another minor."

Network users may not use the Network or any District computer facilities for hate mail, defamatory statements, statements intended to injure or humiliate others by disclosure of personal information (whether true or false), personal attacks on others, and statements expressing animus towards any person or group by reason of race, color, religion, national origin, gender, sexual orientation or disability.

Once adults become involved, it is plain and simple cyber-harassment or cyberstalking. Adult cyber-harassment or cyberstalking is never called cyberbullying.

Users may not send, post, or possess materials that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal, including cyberbullying and "sexting." Users who access such material are expected to discontinue the access as quickly as possible and to report the incident to a supervising teacher and/or technology coordinator.

The best defense for cyberbullying is through education of the minor, parents, and school district personnel.

"Hacking" and Other Illegal Activities

It is a violation to use the School's computer network or the Internet (internally or externally) to gain unauthorized access to other computers or computer systems, or to attempt to gain such unauthorized access. Any use which violates state or federal law relating to copyright, trade secrets, the distribution of

obscene or pornographic materials, or which violates any other applicable law or municipal ordinance, is strictly prohibited.

Confidentiality of Student or Employee Information

Personal information concerning students or employees may not be disclosed or used in any way on the Internet without the permission of a parent or guardian or, if the student or employee is 18 or over, the permission of the student or employee himself/herself. Users should never give out private or confidential information about themselves or others on the Internet, particularly credit card numbers and Social Security numbers. A supervising teacher or administrator may authorize the release of directory information, as defined by Texas law, for internal administrative purposes or approved educational projects and activities.

Legal References

Children's Internet Protection Act of 2000 (H.R. 4577, P.L. 106-554)

Communications Act of 1934, as amended (47 U.S.C. 254[h],[l])

Elementary and Secondary Education Act of 1965, as amended (20 U.S.C. 6801 et seq., Part F)

Citation

Stop Bullying author unknown<http://www.stopcyberbullying.org/what_is_cyberbullying_exactly.html>