District Internet Safety Plan

1. The district is providing Internet access to its employees, board members, and students. The district's Internet system has a limited educational purpose. The district's Internet system has not been established as a public access service or a public forum. The district has the right to place restrictions on use to ensure that use of the system is in accord with its limited educational purpose.

2. Student use of the district's Internet system will be governed by this document, the district's Acceptable Use Policy (AUP), related district and school regulations, and the student disciplinary code. Staff use will be governed by this document, related district policies and regulations, and district employment policy. The due process rights of all users will be respected in the event there is a suspicion of inappropriate use of the district Internet system. Because the law considers information and material on the school network as public documents and requires the monitoring of Internet activity, users should have limited privacy expectations regarding the contents of their personal files and records of their online activity while on the district system.

3. The district Internet system is a limited public forum. The district may restrict access to materials or may place restrictions on student speech for valid educational reasons.

4. This document was developed in accordance with the statutory requirements of the Children's Internet Protection Act (CIPA).

a. The district promotes the effective, educational use of the Internet in school through professional development and the establishment of a district web site that provides access to prescreened, appropriate, and educationally relevant material.

b. Student and staff users of the district Internet system are being educated regularly regarding the safe, ethical, legal, and responsible use of the Internet and of the district's Internet system and their rights and responsibilities under this plan.

c. Student use and activities will be structured in a manner that is appropriate to the age and skills of students.

d. The district protects against access to materials that are considered inappropriate for users to access through the district Internet system in the following manner:

i. The district recognizes that Internet resources can be categorized as prohibited, restricted, limited access, or approved material. Prohibited material may not be accessed by the students or staff at any time, for any purpose. Restricted material may be accessed by students in the context of specific learning activities that have been approved by a teacher or by staff for professional development purposes. Limited access material is material that is generally considered to be non-educational or entertainment. Limited access material may be accessed in the context of specific learning activities that are directed by a teacher or during periods of time that a school may designate as "open access" time. Approved material, on the other hand, can be accessed at all times.

ii. The district has implemented the use of a technology protection measure (filtering software), which is a specific technology that will protect against access to visual depictions that are obscene, child pornography, and materials that are harmful to minors, as defined by CIPA. At the discretion of the district or school, the filtering software may also be configured to protect against access to other material considered inappropriate for student access. The district recognizes, however, that filters are not perfect. They block sites that should not be blocked and let through sites that should be blocked. Therefore, Post ISD does not rely on filters as a sole protection measure. Education on how to handle accidental access, supervision, parental support of policies, and responsible use play important roles.

iii. Authorized staff may temporarily or permanently unblock access to sites containing appropriate material, if access to such sites has been inappropriately blocked by the filtering software.

iv. The determination of whether material is appropriate or inappropriate shall be based on the content of the material and the intended use of the material, not on the protection actions of the filtering software.

e. Student use of the district Internet system will be supervised by staff in a manner that is appropriate to the age of the students and circumstances of use.

f. The district has developed procedures to monitor student use of the Internet through an analysis of Internet usage records.

g. The student AUP includes provisions that address the following safe and responsible use issues:

i. Access to inappropriate material.

ii. Privacy and communication safety standards for self and others

iii. Illegal activities, including computer security violations, actions taken to disrupt the performance of a computer system, and the use of the Internet to engage in other criminal acts.

iv. Inappropriate language.

v. Plagiarism and copyright infringement.

vi. Actions or use that may disrupt or jeopardize the security or effective performance of the district's network or the Internet.

vii. Safety and security when using direct electronic communication

viii. The district follows to guidelines for protecting student personal information when accounts are established on third party web sites in accordance with CIPA.

5. The district will protect against the unauthorized disclosure, use, or dissemination of personal or confidential information of students in accordance with state, federal and local regulations.

6. The district will develop regulations addressing the disclosure of student information, posting student-created material, and posting pictures of students on the district web site.

7. Each school year, parents/guardians must sign an agreement to allow their child to access the Internet.

8. The district educates students to respect intellectual property and observe copyright protection related to material that is accessed through or placed on the Internet.

9. The district has developed district web site guidelines to promote the effective educational use of the Internet, protect the privacy rights and other rights of students and staff, limit potential liability of the district for the inappropriate placement of material, and present an image that will reflect well on the district, schools, staff, and students.

10. The administrative responsibilities of the district administrative staff related to the district Internet system are as follows:

a. The superintendent, or his/her designee, will serve as the coordinator to oversee the district Internet system. The superintendent is authorized to develop regulations and agreements for the use of the district Internet system that are in accord with this plan, and other district policies.

b. The building administrator, or his/her designee, will serve as the building-level coordinators for the district Internet system, and be responsible for interpreting this plan and related regulations at the building level.

c. The district conducts ongoing evaluation of the issues related to this plan, related regulations, and the strategies implemented by schools under this plan.

Guide to Internet Safety

- **Don't give out personal information online.** Keep your name, address, mobile phone number, school name or password a secret.
    - **Don't share personal information online.** You shouldn't give out your personal information to those you don't know because you can't be sure what they will do with it, where it will end up, what it will be used for and who may contact you.
      Sometimes you may have to give your personal information online - for example in registering for new products. The important thing is to remember that this **information can then be passed on to other groups or individuals**. Make sure to investigate who you are providing your information to. **Always check with your parents before giving out information online.**
    - **Don't be fooled by online give-aways or contests!** Often companies will ask you to register with them online because they are interested in selling you something. It's best not to give out too much personal information on forms or quizzes - especially those which ask for personal details of those of other members in your home. Always ask for an adult's opinion if you are unsure.
    - Be careful when filling out "profiles" in clubs of communities. These are public areas of the Internet which people can search on and then contact you.
    - When entering a Chat room you are often asked to give out your AGE, SEX, & LOCATION (ASL). **Stick to your nickname** and don't be too specific about your location.
- Someone you meet in cyberspace can be dangerous! **Never agree to meet someone** you only know online without your parents' permission and then**ONLY** when they are present.

  - **Sadly some young people have met up with people they thought they knew on the internet and have ended up being hurt - or worse.**
  - There are lots of stories about how people have made real friends online and this has obviously involved meeting up face to face after chatting on line. However, it is important to remember that people may not be who they say they are and both young people and adults can be fooled into meeting someone who they might not wish to meet.
  - If a person online asks to meet you – tell your parents or a trusted adult. **Never agree to meet someone alone.** Always take a trusted adult with you for support.
- **Don't open e-mail from someone you don't know.** Opening e-mails or files from people or sources you don't know or trust can get you into serious trouble – these files may contain viruses or nasty messages that once loaded on your computer can cause damage and be very difficult to remove.
  - **Downloads or e-mail can damage your computer and/or include unpleasant pictures or links to web sites with inappropriate content.**
  - If you release personal information about yourself online you may find that you are then bombarded with SPAM or junk mail. Almost everyone receives junk mail or spam – but get smart and reduce your risk. Being careful online means making sure to filter junk e-mail and block individual senders in your e-mail software program.
  - If you receive an e-mail that doesn't have a subject line and carries an attachment – wait to open it until after you have contacted the sender. Make sure you have a anti-virus software protection system on your computer which is up to date. Your virus scanner will not only protect you from receiving viruses but also stop your computer from passing viruses to other users.

- It's important to **remember that someone online may be lying about their real identity**, and information you find on the internet may not be the factual or the truth.
  - You're the boss! It's important to remember that you are in charge when you're online and can choose the people you want to talk to.
  - Be careful as it is difficult to know when someone is pretending and having fun or lying and wanting to be malicious. It is always best to

use caution. If you feel uncomfortable with the way a conversation is going, you have the power to change it:

  - Leave the Chat Room
  - Block contact
  - Report them to your host
  - If someone is aggressive to you about meeting up or making you uncomfortable in **ANY** way, it may be that they aren't the person they say they are. **Don't believe someone online simple because "that's what they said".** They may be lying to you about their age, interests, and even their sex.
  - Individuals are not the only ones who can lie online. Organizations and companies can also be misleading. Don't be afraid to ask questions and check whether information on web sites is true or not.

- **If you ever feel uncomfortable or worried, tell your parents or an adult your trust.**

Cyber Bullying Guide

Students: If you feel you are the victim of bullying, please report it.

School counselors, teachers and administrators will do all they can to help you. Bullying is often a major problem in schoosl.

Cyber Bullying (bullying that takes place on the computer through email or sites such as Facebook, MySpace, etc...) has increased dramatically in the past few years. There are steps that parents can take to help keep their children from becoming victims or from becoming a bully.

Cyberbullying Tips for Parents

- Keep your home computer in easily viewable places, such as a family room or kitchen
- Talk regularly with your child about online activities that he or she is involved in.
- Talk specifically about cyberbullying and encourage your child to tell you immediately if he or she is the victim of cyberbullying, cyberstalking, or other illegal or troublesome online behavior.

- Encourage your child to tell you if he or she is aware of others who may be the victims of such behavior.
- Explain that cyberbullying is harmful and unacceptable behavior. Outline your expectations for responsible online behavior and make it clear that there will be consequences for inappropriate behavior.
- Although adults must respect the privacy of children and youth, concerns for your child's safety may sometimes override these privacy concerns. Tell your child that you may review his or her online communications if you think there is reason for concern.
- Consider installing parental control filtering software and/or tracking programs, but don't rely solely on these tools.
- Contact Law enforcement or Cyber Tipline if:

-You find child pornography on the computer
-Your student has received sexually explicit images or communication.
-Your student has been sexually solicited by someone first met online

*** Keep all evidence

Cyberbullying Tips for Students

KNOW WHAT TO DO WHEN CYBERBULLIED

- Ignore harassing or rude comments posted on your profile
- Save or print the evidence
- Tell an adult you trust
- Try to identify the individual doing the cyberbullying
- Block future contact if possible
- Change your account
- Call the police if the contact involves threats of violence, stalking, child pornography, sexual solicitation, obscene calls or text messages

KNOW HOW TO PREVENT IT

- Only share your password with your parent/guardian
- Change your passwords often
- Set your page and blog to private
- Keep your personal information private

KNOW HOW MUCH IS TOO MUCH

- Use a nickname that doesn't identify your gender, age or location
- Think before posting or sending photos-they could be used to hurt you now and later
- Alter your pictures before you post them to remove identifying information
- Don't post your plans or whereabouts online
- Never meet in person with anyone you meet online
- Think about the real-life consequences of what you post

Post ISD uses training resources from OnGuardOnline.gov. and Kelso's Choice. Printed materials are available at the campus libraries.