Internet Security Tips for Parents and Children

Parents must be educated with respect to the Internet. Be aware of all that it offers:

- Chat Rooms
- E-Mail
- Surfing the Web - search engines
- Posting / Reading messages in newsgroups and bulletin boards.
- Reference information such as news, weather, health issues, sports, stock quotes, movie reviews, encyclopedias, airline reservations, hotel reservations, car rentals, online banking and shopping.

Risks Associated with the Internet:

- Exposure to indecent and/or inappropriate material including sexual, hateful, violent and criminal.
- Child exploitation / molestation
- Harassment
- Financial fraud

What Parents can do to reduce the risks associated with the Internet:

- Get involved with your children. Find out what they are doing and where they are going on the internet.
- Teach your children about the dangers of the Internet and how to avoid them.
- Consider software programs that block and filter inappropriate websites.
- Place the computer in an area of the house that is easily visible so that you can periodically check to see what your child is doing.
- Watch for warning signs such as your child spending large amounts of time online, especially at night; you find pornography on the computer or disks/cd's; your child receives phone calls from men you don't know or from numbers you don't recognize including long distance, or your child receives mail, gifts or packages from unknown sources.
- Consider signing a "Family Contract for Online Safety" which includes a "Kids" and a "Parents" pledge (available hand-out).

School Safety Guidelines for the Internet

1. A unique sign-on and password should be provided to each user that is not easily guessed. Impress upon the student the importance of keeping their password secret.
2. Student names and sign-on names should be recorded in a log securely maintained by the school computer room monitor each time a student is granted permission to use a computer.
3. This log should also contain the unique designation for the computer the student is assigned to.
4. No swapping of assigned computers should be permitted unless there is a technical difficulty.
5. Computers should be programmed to sign off after a short period of inactivity requiring the student to sign back on. This prevents a second student from using a computer already signed on by a different student.
6. Install video surveillance that is time coded, to show the activity at all the student computers. If video surveillance is impractical for some circumstances then a monitor should visually oversee the activities of the students on the computers. This establishes a record of which student was using a particular computer at a particular time.
7. Servers and firewalls should be maintained in a secure area with limited access.
8. Logging should be set on the servers/firewalls so that identification can be made at a later date as to what computer was used at a certain time to access e-mail or the internet.
9. Video surveillance should also be maintained on the servers/firewall.
10. No student should be allowed to install software or data files on a computer without authorization.
11. A strong virus protection program must be installed and upgraded daily.
12. Computer room monitors should be actively overseeing the content of the programs being used by the students.
13. A banner should appear prior to sign-on that requires the user to acknowledge that the computer is not for personal use and that all information on the computer is property of the school district, and any unauthorized access is illegal.
14. Scheduled backups should be maintained in a secure facility away from the server/firewall and reviewed to assure it is accurate.
15. Review server/firewall logs in a timely fashion so that intrusion attempts or unauthorized access can be addressed immediately.
16. Software should include password verification programming to eliminate duplicated or overly simplistic passwords.