

# KEEPING YOUR CHILD SAFE ONLINE

VOLUME 1, ISSUE 1  
FALL 2007

William Jefferson Clinton Middle School



## Tips to keep your child safe online

- Keep any computer in a public area; do not let your child keep his/her computer in the bedroom.
- Learn how to read the computer screen including minimized programs and online chat services.
- Use the online chat software to view previous messages/discussions on your child's screen name(s).
- Help your child to create a screen name that is gender neutral and does not mention your child's age or level of education.
- Make sure your child deletes all profiles that he/she may have online that could reveal age, location, school, etc...
- Get your own account for instant messengers, MySpace.com, Second-Life, and any other program your child uses that requires signing on for certain privileges.
- And most important! Learn about your computer! The more you know, the less your child can keep hidden from you. It's OK to look around the web and see what's out there. It's OK to open the files on your computer to see what your child is doing. What is more important? Your child's "right to privacy" or your child's safety?

### For more information...

<http://www.netSMARTZ.org/>

[http://kidshealth.org/parent/positive/family/net\\_safety.html](http://kidshealth.org/parent/positive/family/net_safety.html)

<http://www.safekids.com/>

<http://www.internet-safety.org/index.htm>

<http://www.cyberbee.com/safety.html>

## Facts About the Acceptable Use Policy (AUP)

- Each student must turn in an AUP with his/her signature and a parent's signature before he/she can use any computers on a school site. This form must be filled out each year.
- Students who violate the AUP can be suspended and even expelled from school.
- The AUP outlines all of the rules that students must follow as they use the computers on campus including, but not limited to: sending and receiving files/email, posting messages, visiting websites, staying off of banned sites, staying off of proxy servers, not creating/sending viruses and worms, etc...

## CYBERBULLYING

Many students ask why sites like MySpace.com are blocked at the school site. One of the reasons is cyberbullying. Cyberbullying is becoming more and more prevalent in our country each year.

As children become more technologically aware, they also become more dangerous to each other. Each day, thousands of children are the victims of cyber-bullies. These bullies hit children emotionally rather than physically. And each year, the number of suicides attributed to the effects of cyberbullying grows.

What is cyberbullying? Cyberbullying is the use of tech-

nology to harm someone by sending hateful messages directly to him/her on a cell phone or by an Instant Message, and/or posting pictures or messages about the person who is being bullied.

Often, these message are sent using an Instant Message service like Yahoo! Messenger or AOL Instant Messenger (AIM). However, sites like MySpace.com are also used.

A student might post a picture of him/herself on a MySpace site that is shared among friends. A cyberbully will take that picture, manipulate it, "morph" it, and/or write messages on the picture then re-post it for

all to see.

These kinds of actions are damaging to young students and are intentionally designed to cause as much emotional damage as possible.

For these reasons and more, sites like MySpace.com will continue to be blocked at the school site.

Please help your children to learn that this kind of activity is dangerous and wrong. Watch your child to see if he/she has been the victim of cyberbullies and report any cyberbullying of any kind to your child's school site at once.

We want our children to feel safe online both at school and at home.

## SOME INTERNET VOCABULARY

**Phishing** is when a website is created to look like a site from an established company like your bank or your internet service provider (ISP). After it is created, emails are randomly sent out to addresses around the world that have a link to the fraudulent site. The hope of the sender is that people will take the "bait", connect to the site, and input private information like social security numbers, credit card numbers,

bank account numbers, passwords, etc. Once entered, this information becomes available for the criminal to use to commit cyber-crimes.

**Protect yourself:** Don't click on any link to a site that requests personal information. Your internet company and/or bank will never ask for your password when sending an email. If you do link to a site that requests this information, get off of it immediately.

**Spam** is the email that

comes from various sites to sell products or advertise sites online. These emails often come after a person has signed up for information on a website. They may also contain viruses or worms that can harm your computer.

**Protect yourself:** Create a second email account that you only use when visiting websites. Do not give out the address to your main email account to anyone except friends and family.