

# Safeguarding Against Inappropriate Websites

*Copied from Church media articles*

There is no such thing as a right to privacy when it comes to patrolling what comes into your homes via the Internet or any other means. Parents have a right and a sacred duty to protect their homes and their children from any unwanted influence that may assault them.

\* Place your computer in an open access area.

Having the computer in sight reminds everyone in the family to be careful about the information they access. It also makes it harder to view things that may be inappropriate when it's out in the open.

\* Regulate hours on computers. Be careful in using the computer alone or late at night.

\* Use a password for your computer. This way, parents will have to log on to the Internet for their children and retain control of its use.

\* Talk candidly with your children about the Internet.

Don't be afraid to ask questions and establish an open communication where children can feel comfortable talking with you. Ask about past experience with the Internet.

One thing to remember is that if a child has been accidentally exposed to porn they may feel guilty about the experience. Let them know that it isn't their fault and that they were an innocent victim.

\* Bookmark child-friendly web sites.

Internet browsers have a feature that lets you mark sites that you wish to visit often. It's usually an option on the top of the menu called 'bookmark' or 'favorites.'

Marking a selection of sites gives your children a good choice of places to visit when they use the Internet.

\* Teach children to avoid giving out personal information.

Establish some house rules about what information can and cannot be shared on the Internet. Information such as street address, telephone number, credit card information and even e-mail addresses should not be shared without first gaining parental approval.

\* Check your web browser history regularly.

Internet browsers keep a history on your computer of which sites have been visited. There are at least four places on the computer where information is stored from web sites. Most web browsers have a history button or an option on the menu to let you browse through a list of web sites that have been visited.

Internet Explorer has the button, Netscape's history is listed in the tools menu.

There is another trail of information stored on your computer. These are files that are left by the sites you visit and help in the performance of the web site next time you visit.

These "cookies" can be found in the tools menu. Choose "Internet options" and look for "temporary Internet files" section. Click "settings" and look for "view files" button. This will open a window showing the files left by the different web sites.

Look at the column labeled 'Internet address.' This is the web address where these files came from. From the names in the web address, you can usually determine the purpose of the site. You can set the number of days to keep history files. If there are no files listed, then someone may have chosen to clear the history. This is one way to hide where they have been browsing.

**Know the parents of your children's friends.**

Your children may use a computer at their friends' homes or other places. Talk with your children's friends' parents to find out what rules they use regarding the Internet.

Knowing the parents help you become familiar with their family's entertainment standards.

Know that even though your children may be protected in your home, they may not be as safe at a friend's.

**\* Ask your Internet Service Provider (ISP) about filters to block web sites.**

Some ISPs provide filters to block information parents deem inappropriate. If your ISP doesn't, you can install software on your computer to do so.

There are two types of filtering services available. Server based filtering and PC based filtering both have advantages and disadvantages.

It is important that you know that these filters are not perfect and won't block all bad sites.

Ultimately, the best Internet filter is the parents.

**\* Share your learning with others.**

Talk with your family and friends about what you have discovered as you have searched the web, ask them how they have avoided inappropriate sites.

Also find out what sites have been especially beneficial.

**\* Stay out of public chat rooms.**

Would you ever turn your child loose in big city late at night and say 'Hey, go look around and see if you can find a new friend?'

This is just what's happening when children are allowed to chat in chat rooms unsupervised.

One reason pedophiles are particularly fond of the Internet is because they think they are anonymous, They use the chat rooms and e-mail exchange information and pornography to interact with children.

Use only private (user ID & password protected) chat rooms with friends & relatives who you and your children know well.

Beware of public computer bulletin boards that may lure children in with games and establish relationships and try to arrange face-to-face contact.

**\* Teach children to crash and tell.**

Teach your children that if they bring up a bad picture on the Internet, they should immediately turn off the computer. Many pornography sites use a technique called 'mouse trapping,' which locks you into their web site. As you attempt to exit the site, another window will appear on the screen. Each new window will expose a child to more and more pictures. Some will even change your computer's home screen.

There is very little risk of damage to your computer by turning it off. Computer hardware and software is designed to handle power failures.

The red button on the surge protector is a good button to teach children to use. Afterward, have them tell you so you can check the computer's system to make sure that the home page was not changed.

A computer with an Internet connection provides the doorway to an online world of libraries, museums, business, school and people all willing to talk with you. The Internet is an exciting place, but we need to be on guard.