Your Family and Internet Safety: Creating a Usage Policy

Introduction

A typical teenage girl, Natalie does well in school, plays clarinet in the school band, and like many girls her age, spends much of her time talking to friends in online chat rooms.

One night, Natalie is using her city's chat room when she gets an instant message from a girl she's never met before. Natalie, knowing full well the dangers of being online, never gives out her last name, her address, pictures of herself, nor her phone number to people she doesn't know online, this stranger included. Her new online friend, however, sends Natalie a picture of herself, and upon seeing that they're about the same age, Natalie's guard comes down a little. The two begin to chat about being in the school band, what grade they're in, and their schools in general. After a short while, Natalie's new online friend says she has to go and that she hopes to talk to her again soon. They say goodbye and Natalie goes back to talking to her friends.

The next afternoon there's a knock at the door of Natalie's house. Natalie's mother opens the door to find a policeman standing there asking to speak with her. He says that last night he spoke with Natalie in an Internet chat room while posing as a teenage girl and asks her mother if she's spoken to her daughter about the dangers of talking to people online. Her mother says that she's told Natalie never to give out her last name, her address, phone number, etc. to anyone she doesn't know. The officer says that Natalie never did give out any of that information, but by finding out what high school she goes to, what grade she's in, and what instrument she plays in the band, he was able to get her last name and address with the help of a school yearbook and a phone book.

> *… by finding out what high school she goes to, what grade she's in, and what instrument she plays in the band, the officer was able to get her last name and address with the help of a school yearbook and a phone book.*

The Internet is, perhaps, one of the greatest inventions of all time. Where else can one find information on the most obscure subject, instantly, from anywhere in the world? It has revolutionized how we as a society educate, do business, and communicate, and as more and more people connect to the Internet on a daily basis, the more we can learn and grow as individuals and as a culture.

However, the Internet has its own dangers and there are people out there who use it for the wrong reasons.

PURDUE
UNIVERSITY

CERIAS The Center for Education and Research in Information Assurance and Security

Purdue University ● 656 Oval Drive ● West Lafayette, IN● 47907-2086
(765) 494-7871● Fax (765) 496-3181● k-12@cerias.purdue.edu ● www.cerias.purdue.edu

As adults we are able to make our own informed decisions about how to spend our time online, but our children require much more guidance and assistance.

The first thing that comes to mind when thinking of online safety is often protection from offensive websites,. There are over 250 pornographic websites created each day, which adds to the over 75,000 already out there. Besides pornography, there are thousands upon thousands of sites on the Internet that contain hate material directed toward people of different races or religious beliefs or sites that promote violence, terrorism or drug use, with many of these sites instructing readers how to build weapons or make drugs in the privacy of their own homes.

But online safety is about much more than offensive websites. Issues such as identity theft, child predation, and harassment are only a few of the darker aspects of the online age. Perhaps the greatest threat to our daily lives is identity theft. Sometimes through a simple Internet search on Google or Yahoo, one can quickly find a person's full name, home address, phone number, parents' names, social security number, etc., and easily fill out credit card applications or make purchases without their knowledge.

Harassment is also very prevalent online. One out of every five kids using the Internet is approached for sex either by email or through chat rooms and instant messaging, and since teens now spend an average of 8.5 hours a week in chats or using email as opposed to 1.5 hours a week using the Internet for school work, this number will only rise.

Financial threats can also be found online. Yes, identity theft can lead to financial trouble, but don't forget about children with a parent's credit card information! Even if your child doesn't have access to a credit card, there are now Internet services that can be paid through the phone bill, not unlike 1-900 numbers, but far more expensive.

> *While on AOL, not an hour went by when I wasn't sent an annoying instant message from someone asking me how old I am, where I live, what my sexual preference is and so on. From time to time the messages would just be down right disgusting. Consistent harassment was enough to make me change my server. I just wanted more privacy while doing research or writing emails.*
>
> Janna—St. Paul, MN

What to do

The good news about facing the dangers of the Internet is that there are many options out there for dealing with these obstacles. The bad news about facing the dangers of the Internet is that there are many options out there for dealing with these obstacles. It truly is a double-edged sword. There is just so much material and software and myths and lies concerning threats to families while online that it's difficult to make heads or tails out of it.

PURDUE
UNIVERSITY

The Center for Education and Research in Information Assurance and Security

Purdue University ● 656 Oval Drive ● West Lafayette, IN● 47907-2086
(765) 494-7871 ● Fax (765) 496-3181● k-12@cerias.purdue.edu ● www.cerias.purdue.edu

Luckily the plan of attack for combating the dangers of the online world can be put into two easy categories—prevention and collaboration. Prevention includes the technical and non-technical solutions to the issue of protection, while collaboration is concerned with keeping an open dialogue between parent and child about using the Internet so they feel safe and comfortable to come to you for questions or issues.

> *Prevention includes the technical and non-technical solutions to the issue of protection, while **collaboration** is concerned with keeping an open dialogue between parent and child…*

Once these two categories have been fully discussed, the information learned from them can be used to create a home Internet usage policy for you and your family, which spells out exactly what can and cannot be done while online and the consequences for not following it fully.

Prevention

There are four main steps when it comes to the prevention of online problems—**building good boundaries, avoiding trouble spots, maintaining oversight,** and **setting a good example**.

> *The four keys to prevention are **building good boundaries, avoiding trouble spots, maintaining oversight,** and **setting a good example.***

Building good boundaries is a three-step process. First, it's all about location, location, location. The computer should always be in a high-traffic area of the house and never in the child's bedroom. This way you can casually stroll by and see what your child is up to while online rather than banging on the bedroom door and checking for pornography. If your child constantly minimizes windows as you pass, you know something's up.

The second boundary involves setting time restrictions. Remember that children spend on average 8.5 hours a week in chat rooms or sending email while only spending 1.5 hours doing school work online. Setting consistent time limits and scheduling when your child can be online and for what reason will help make sure your child is online for the right reasons.

The third boundary is a technical one. There are many products out on the market today that can help protect you and your children from many of the dangers of being online, with some being more complicated than others.

On the more inexpensive, non-high-tech side, many of these technological boundaries come with your own Internet service provider (ISP). AOL keyword "parental controls" is a good example of this, which allows you to set specific rules for content, messaging, email, etc. for the whole family. It's also a good idea to have separate email accounts for sending email to

PURDUE
UNIVERSITY

The Center for Education and Research in Information Assurance and Security

Purdue University ● 656 Oval Drive ● West Lafayette, IN● 47907-2086
(765) 494-7871 ● Fax (765) 496-3181● k-12@cerias.purdue.edu ● www.cerias.purdue.edu

friends and family and for sending email to companies and email lists to help keep the SPAM in one location. There are also family filters on search engines and special search engines just for kids. Yahooligans.com automatically filters out websites of a questionable nature so kids can look up information safely, while lycos.com and google.com have password-protected safeguards that filter out what you specifically tell it to filter out for safer searching.

On the more advanced side of the technological boundary, there are many programs that can be bought today to help assist in filtering content. Remember, however, that these should only be bought in order to assist you in protecting your child, not act as a babysitter. Although seventy-one percent of parents stop supervising Internet use by their kids after age fourteen, seventy-two percent of all net-related missing children are fifteen or older.

It's important that any filtering software you purchase is as customizable to your needs as possible. Look for software that allows you to filter out a variety of website content for your children, block specific newsgroups, email, and unmonitored chat rooms, and manages time spent online.

Although there are many filters on the market today that can protect in many different ways, www.filteringreview.com can help you make better sense of everything that's out there with reviews by people who use the products and lists of what each product includes. It's a great place to start before you head out to the store and buy something that doesn't work as well as you hoped.

Once good boundaries have been established, it's important to still **avoid the trouble spots**. Even if you don't buy filtering software, you can still take steps like having your children avoid unmonitored newsgroups and unfiltered searches. Also make sure they stay out of unmonitored chat rooms and keep themselves from talking to people they don't know on messaging programs.

Maintaining oversight involves checking up on your child's Internet activity once they've stopped using it, which is done through checking the history folder and the cookies of the web browser.

Setting a good example is all about doing as you say *and* as you do. If your child sees you downloading music for free or looking at adult websites or minimizing windows every time they come in the room, they're going to feel that it's alright for them to do just the same.

PURDUE
UNIVERSITY

The Center for Education and Research in Information Assurance and Security

Purdue University ● 656 Oval Drive ● West Lafayette, IN● 47907-2086
(765) 494-7871 ● Fax (765) 496-3181● k-12@cerias.purdue.edu ● www.cerias.purdue.edu

Collaboration

It's essential that you always keep a dialogue with your child about their use of the Internet, and there are three ways to go about doing this—**open communication, constructive activities,** and **balanced use of time.**

Open communication involves simply asking what your children do while online, from playing games to working on their homework. Ask your children about whom they talk to while online or send email to, and especially encourage them to always come to you if they have questions or concerns about things that happen while they are online.

Open communication also means talking to teachers and administrators at your child's school as well. Although it seems drastic, remember that student Internet use at school has more than tripled since 1997, meaning that children are more likely to be online at school now than at home, and for longer periods of time. Ask teachers and administrators how much they watch their students to make sure they're not going anywhere they're not supposed to be going or how the Internet is used in classes. Most schools today have a usage policy that they have students and parents sign; ask for one if you haven't seen one or request that one be written up so both you and your child know what is expected of them at school.

Kids are in such a hurry to grow up that they will sometimes pretend to be older than they are when they are online. I worry that this kind of behavior, while normal, could lead to a dangerous or harmful situation down the road.

Michael—Greensboro, NC

Talk with your children about privacy. Explain how no one should be able to know names, addresses, phone numbers, social security numbers, etc., and to always ask you before giving any such information out to anyone while online.

Put it into "real-world" terms—it's no different than walking up to any random person on the street and telling that person your life story.

Sexual harassment and exploitation is a subject that no parent wants to think about, but it's a subject that has to be brought up before something possibly happens. There are three steps to take when confronted with this type of incident. First, it's important to identify the problem. There's a big difference between a fellow student making comments and a sexual predator looking to take pictures, so make sure you know exactly what's going on. Also make sure to tell the child that it's just as important to inform you of SPAM and inappropriate websites as it is to inform you about people on instant messenger and in chat rooms. Once you've determined what happened online, and it's something serious, it should

The Center for Education and Research in Information Assurance and Security

Purdue University ● 656 Oval Drive ● West Lafayette, IN● 47907-2086
(765) 494-7871● Fax (765) 496-3181● k-12@cerias.purdue.edu ● www.cerias.purdue.edu

be reported immediately. Since there is no Internet law enforcement, the first people to contact would be your local police and work from there. After the situation has been dealt with, it's important to conclude with talking with the child about how to avoid such an instance in the future.

Constructive activities take open communication to the next level as you sit down at the computer with your child and show them how to navigate the Internet safely, free from incident. Show them websites that are safe for kids to use as you highlight both good and bad content. Go on virtual field trips with your child so they can learn more about subjects that they're discussing in classes. Work on the family's web page together so they can learn more about web publishing and the mechanics of the Internet—it's best to get children online as soon as they can move a mouse.

It's always best to remember to keep a **balanced use of time** when it comes to using the Internet in everyday life. Remember that the computer is not a babysitter but a tool. You wouldn't leave your child unattended in the garage while you were doing something else, so why would you leave him sitting alone on a computer? Be sure to remind children that there is an entire world outside the door because it's a little difficult to get exercise and sun while sitting at a computer. Finally, set limits and stand by them. If you tell your child that he can only be online for an hour, then make sure he's only online for an hour.

> *I worry that my daughter will learn things like the truth about Santa Claus and other sweet, innocent beliefs that a child loves to experience. I mean, don't get me wrong, I am also worried about the usual internet stalkers and porn, but, if I keep a block on those sites for her and do my part, then, I hope that lessens the chance of her exposure.*
>
> Jennifer—Flower Mound, TX

In order to keep to these rules and combine prevention and collaboration, the best solution is to create a home Internet usage policy.

Creating a home Internet usage policy

When a company wants to make sure their employees are doing what they are supposed to be doing while online at work, they have what is referred to as a usage policy. Similar to a contract, a usage policy states what one should and shouldn't do while online and the consequences for not following that policy.

> *A home-centered Internet usage policy should be a well-balanced combination of both prevention and collaboration...*

This same idea can be used in the home environment as well. A home-centered Internet usage policy should be a well-balanced combination of both prevention and collaboration, which contains

The Center for Education and Research in Information Assurance and Security

Purdue University ● 656 Oval Drive ● West Lafayette, IN● 47907-2086
(765) 494-7871 ● Fax (765) 496-3181● k-12@cerias.purdue.edu ● www.cerias.purdue.edu

specifics on how the Internet is to be used at home and the results of not following those specifics.

What makes it more difficult for you as a parent is writing this policy in a way appropriate for your children. Kids at different ages use the Internet for different reasons, and it's important that you observe your children as they spend time online to see just what they are using it for.

Even though kids use the Internet for different reasons, the fundamental rules remain the same:

- Never give out **any** type of personal information.
- Always abide by the "Golden Rule" when in chat rooms, talking on instant messenger, or sending email—treat others the way you'd wish to be treated.
- Never meet or call people that you've only ever talked to online without parental permission or supervision.
- Always report suspicious activity to those in authority.
- The prohibition of the viewing of certain websites or going to sites of a questionable nature without parental consent.
- Not purchasing things online without parental consent.
- Setting time limits for using the Internet as play time.
- Never open email attachments you're not expecting because they could contain viruses, whether you know the sender or not.
- Never use file sharing programs because they're both illegal and often rampant with viruses.

Also be sure to include parent responsibilities, such as:

- Asking your children about their online friends and what sites they go to.
- Not to overreact when the child comes to you for help, advice, or concern.
- Setting up time when both of you can use the Internet together.

It's also important to stress that this policy applies to home, school, and at friends' homes.

Once the rules have been laid out, both you and your child should decide upon appropriate consequences for not following the rules. This could include complete prohibition from the computer or the Internet, loss of the use of instant messaging programs or chat rooms, games, etc.

The Center for Education and Research in Information Assurance and Security

Purdue University ● 656 Oval Drive ● West Lafayette, IN● 47907-2086
(765) 494-7871● Fax (765) 496-3181● k-12@cerias.purdue.edu ● www.cerias.purdue.edu

Once you've completed your policy, have both of you sign it and post it in a location near the computer where it can always be seen.

Summary

Although software and policies are certainly helpful in preventing children from participating in questionable activities, they can't fully protect children from all the dangers of the Internet. Children ultimately have to make these decisions on their own, but with good parental guidance and models, the chance of harm coming to either your child or your computer will be greatly reduced.

For further information

To learn more about safely using the Internet, please visit the following websites:

www.cerias.purdue.edu/education/k-12
www.getnetwise.org
www.staysafeonline.info

The Center for Education and Research in Information Assurance and Security

Purdue University ● 656 Oval Drive ● West Lafayette, IN● 47907-2086
(765) 494-7871 ● Fax (765) 496-3181● k-12@cerias.purdue.edu ● www.cerias.purdue.edu