

# Internet Safety



**Internet use is growing enormously every day. What does this mean for parents?**

Here is some information about how Coventry Local Schools works to make exploring the Internet safe and educational in our schools, followed by information taken from a brochure, "A Parent's Guide to Internet Safety", created by the FBI.

## **Computer Safety and Coventry Local Schools**

Coventry Local Schools employs a number of measures designed to create safe educational use of school computers and other communication devices by both students and staff. The district uses a filtering system to block student access to known objectionable sites. This filtering system is constantly being updated to include sites springing up at any time that are deemed inappropriate for students and/or staff to visit.

Given the vastness of the Internet, no filtering system guarantees an ability to filter ALL harmful sites. Therefore, CLS students and staff are actively encouraged to report objectionable sites to school officials who can add such sites to those blocked by CLS. Also, staff is required to monitor student usage of school computers.

Students and staff sign Internet use agreement documents that govern acceptable use of school computers. Violations of the district's acceptable use policies can result in revoking a user's privileges to use the district's electronic equipment. If a violation of law has occurred, the district will turn such information over to the appropriate law enforcement agency.

With the evolution of computing devices to include cell phones, personal digital assistants (PDAs), and even some video-gaming systems, the district's policy extends to the use of any of these devices while on school property at the Middle School and High School for EDUCATIONAL PURPOSES and with the teacher's or administrator's permission. Though a student's cell phone is private property, misuse of that device at school can result in confiscation of the phone that then has to be retrieved either at the school or at the district's central security department.

The power of the Internet as a learning resource cannot be overstated. But like all powerful technologies or tools, there can be dangers associated with use of the resource. Keeping students safe while they are becoming educated is an overriding priority of Coventry Local Schools. So the district wants to be proactive in helping educate parents about computer use not only while students are supervised in school but also when they may go on-line at home, or other non-school location.

There are many resources available to parents that provide information, good advice, and guidance for dealing with student exploration of the Internet and other communication vehicles. Millions of students go on-line every day, and most are safe. The way to stay safe is to

understand the dangers and follow some simple rules for keeping out of trouble.

Here are just a few resources worth checking out by both students and parents:

[www.cybertipline.com/](http://www.cybertipline.com/) (National Center for Missing & Exploited Children) 1-800-843-5678

[www.fbi.gov/innocent.htm](http://www.fbi.gov/innocent.htm)

[www.safekids.com/](http://www.safekids.com/)

[www.safeteens.com/](http://www.safeteens.com/)

[www.ikeepsafe.org/](http://www.ikeepsafe.org/)

### **A Parent's Guide To Internet Safety**

(The following information is provided by the U. S. Department of Justice - Federal Bureau of Investigation)

#### **Computer Sex-Offenders**

While on-line computer exploration opens a world of possibilities for children, expanding their horizons and exposing them to different cultures and ways of life, they can be exposed to dangers as they hit the road exploring the information highway. There are individuals who attempt to sexually exploit children through the use of on-line services and the Internet. Some of these individuals gradually seduce their targets through the use of attention, affection, kindness, and even gifts. These individuals are often willing to devote considerable amounts of time, money, and energy in this process. They listen to and empathize with the problems of children. They will be aware of the latest music, hobbies, and interests of children. These individuals attempt to gradually lower children's inhibitions by slowly introducing sexual context and content into their conversations.

There are other individuals, however, who immediately engage in sexually explicit conversation with children. Some offenders primarily collect and trade child pornographic images, while others seek face-to-face meetings with children via on-line contacts. It is important for parents to understand that children can be indirectly victimized through conversation, i.e. "chat," as well as the transfer of sexually explicit information and material. Computer-sex offenders may also be evaluating children they come in contact with on-line for future face-to-face contact and direct victimization. Parents and children should remember that a computer-sex offender can be any age or sex the person does not have to fit the caricature of a dirty, unkempt, older man wearing a raincoat to be someone who could harm a child.

Children, especially adolescents, are sometimes interested in and curious about sexuality and sexually explicit material. They may be moving away from the total control of parents and seeking to establish new relationships outside their family. Because they may be curious, children/adolescents sometimes use their on-line access to actively seek out such materials and

individuals. Sex offenders targeting children will use and exploit these characteristics and needs. Some adolescent children may also be attracted to and lured by on-line offenders closer to their age who, although not technically child molesters, may be dangerous. Nevertheless, they have been seduced and manipulated by a clever offender and do not fully understand or recognize the potential danger of these contacts.

### **What Are Signs That Your Child Might Be At Risk On-line?**

**Your child spends large amounts of time on-line, especially at night.**

Most children that fall victim to computer-sex offenders spend large amounts of time online, particularly in chat rooms. They may go on-line after dinner and on the weekends. They may be latchkey kids whose parents have told them to stay at home after school. They go on-line to chat with friends, make new friends, pass time, and sometimes look for sexually explicit information. While much of the knowledge and experience gained may be valuable, parents should consider monitoring the amount of time spent on-line.

Children on-line are at the greatest risk during the evening hours. While offenders are on-line around the clock, most work during the day and spend their evenings on-line trying to locate and lure children or seeking pornography.

**You find pornography on your child's computer.**

Pornography is often used in the sexual victimization of children. Sex offenders often supply their potential victims with pornography as a means of opening sexual discussions and for seduction. Child pornography may be used to show the child victim that sex between children and adults is "normal." Parents should be conscious of the fact that a child may hide the pornographic files on diskettes from them. This may be especially true if other family members use the computer.

**Your child receives phone calls from men you don't know or is making calls, sometimes long distance, to numbers you don't recognize.**

While talking to a child victim on-line is a thrill for a computer-sex offender, it can be very cumbersome. Most want to talk to the children on the telephone. They often engage in "phone sex" with the children and often seek to set up an actual meeting for real sex.

While a child may be hesitant to give out his/her home phone number, the computer-sex offenders will give out theirs. With Caller ID, they can readily find out the child's phone number. Some computer-sex offenders have even obtained toll-free 800 numbers, so that their potential victims can call them without their parents finding out. Others will tell the child to call collect. Both of these methods result in the computer-sex offender being able to find out the child's phone number.

**Your child receives mail, gifts, or packages from someone you don't know.**

As part of the seduction process, it is common for offenders to send letters, photographs, and all manner of gifts to their potential victims. Computer-sex offenders have even sent plane tickets in

order for the child to travel across the country to meet them.

**Your child turns the computer monitor off or quickly changes the screen on the monitor when you come into the room.**

A child looking at pornographic images or having sexually explicit conversations does not want you to see it on the screen.

**Your child becomes withdrawn from the family.**

Computer-sex offenders will work very hard at driving a wedge between a child and their family or at exploiting their relationship. They will accentuate any minor problems at home that the child might have. Children may also become withdrawn after sexual victimization.

**Your child is using an on-line account belonging to someone else.**

Even if you don't subscribe to an on-line service or Internet service, your child may meet an offender while on-line at a friend's house or the library. Most computers come preloaded with on-line and/or Internet software. Computer-sex offenders will sometimes provide potential victims with a computer account for communications with them.

#### **What Should You Do If You Suspect Your Child Is Communicating With A Sexual Predator On-line?**

- Consider talking openly with your child about your suspicions. Tell them about the dangers of computer-sex offenders.
- Review what is on your child's computer. If you don't know how, ask a friend, coworker, relative, or other knowledgeable person. Pornography or any kind of sexual communication can be a warning sign.
- Use the Caller ID service to determine who is calling your child. Most telephone companies that offer Caller ID also offer a service that allows you to block your number from appearing on someone else's Caller ID. Telephone companies also offer an additional service feature that rejects incoming calls that you block. This rejection feature prevents computer-sex offenders or anyone else from calling your home anonymously.
- Devices can be purchased that show telephone numbers that have been dialed from your home phone. Additionally, the last number called from your home phone can be retrieved provided that the telephone is equipped with a redial feature. You will also need a telephone pager to complete this retrieval. This is done using a numeric-display pager and another phone that is on the same line as the first phone with the redial feature. Using the two phones and the pager, a call is placed from the second phone to the pager. When the paging terminal beeps for you to enter a telephone number, you press the redial button on the first (or suspect) phone. The last number called from that phone will then be displayed on the pager.
- Monitor your child's access to all types of live electronic communications (i.e., chat rooms, instant messages, Internet Relay Chat, etc.), and monitor your child's e-mail. Computer-sex offenders almost always meet potential victims via chat rooms. After meeting a child on-line, they will continue to communicate electronically often via e-mail.

**When should you immediately contact local/state police, the FBI, and the National Center for Missing and Exploited Children?**

- Your child or anyone in the household has received child pornography.
- Your child has been sexually solicited by someone who knows that your child is under 18 years of age.
- Your child has received sexually explicit images from someone that knows your child is under the age of 18.

If any of these scenarios occurs, keep the computer turned off in order to preserve any evidence for future law enforcement use. Unless directed to do so by the law enforcement agency, you should not attempt to copy any of the images and/or text found on the computer.

**What Can You Do To Minimize The Chances Of An On-line Exploiter Victimized Your Child?**

- Talk to your child about sexual victimization and potential on-line danger.
- Spend time with your children on-line. Have them teach you about their favorite on-line destinations.
- Keep the computer in a common room in the house, not in your child's bedroom. It is much more difficult for a computer-sex offender to communicate with a child when the computer screen is visible to a parent or another member of the household.
- Use parental controls provided by your service provider and/or blocking software. While electronic chat can be a great place for children to make new friends and discuss various topics of interest, it is also prowled by computer-sex offenders. Use of chat rooms, in particular, should be heavily monitored. While parents should utilize these mechanisms, they should not totally rely on them.
- Always maintain access to your child's on-line account and randomly check his/her email. Be aware that your child could be contacted through the U.S. Mail. Be up front with your child about your access and reasons why.
- Teach your child the responsible use of the resources on-line. There is much more to the on-line experience than chat rooms.
- Find out what computer safeguards are utilized by your child's school, the public library, and at the homes of your child's friends. These are all places, outside your normal supervision, where your child could encounter an on-line predator.
- Understand, even if your child was a willing participant in any form of sexual exploitation, that he/she is not at fault and is the victim. The offender always bears the complete responsibility for his or her actions.
- Instruct your children that they should NEVER:
  - Arrange a face-to-face meeting with someone they met on-line;
  - Upload (post) pictures of themselves onto the Internet or on-line service to people they do not personally know;
  - Give out identifying information such as their name, home address, school name, or telephone number;
  - Download pictures from an unknown source, as there is a good chance there could be sexually explicit images;

- Respond to messages or bulletin board postings that are suggestive, obscene, belligerent, or harassing.
- Remind your child often that whatever they are told online may or may not be true.

### **Frequently Asked Questions:**

#### **My child has received an e-mail advertising for a pornographic website, what should I do?**

Generally, advertising for an adult, pornographic website that is sent to an e-mail address does not violate federal law or the current laws of most states. In some states it may be a violation of law if the sender knows the recipient is under the age of 18. Such advertising can be reported to your service provider and, if known, the service provider of the originator. It can also be reported to your state and federal legislators, so they can be made aware of the extent of the problem.

#### **Is any service safer than the others?**

Sex offenders have contacted children via most of the major on-line services and the Internet. The most important factors in keeping your child safe on-line are the utilization of appropriate blocking software and/or parental controls, along with open, honest discussions with your child, monitoring his/her on-line activity, and following the tips in this pamphlet.

#### **Should I just forbid my child from going on-line?**

There are dangers in every part of our society. By educating your children to these dangers and taking appropriate steps to protect them, they can benefit from the wealth of information now available on-line.