

Instructions for Parents, Guardians, Educators, and Other Caring Adults

Junior High Level, Grades 6, 7, 8 (ages 11 to 14 years)

Lesson Plan 7: Internet Safety

Getting started with Lessons 7:

Principle:	 Educating children about Internet Safety. Specifically: Some Do's and Don'ts of interacting with people on the Internet, and The importance of protecting yourself and your personal information while using the Internet.
Catechism:	Man is obliged to follow the moral law, which urges him "to do what is good and avoid what is evil" (cf. GS 16). This law makes itself heard in his conscience. #1713
Goal:	To assist children and young people in recognizing the risks of providing personal information to anyone on the Internet and to help them realize how hard it is to know who someone really is when the only avenue of communication is the Internet.
Objectives:	To teach children and young people safety rules for the Internet and to raise children and young people's awareness about the ways adults can use the Internet to confuse and "trick" them into believing things that are not true. The goal for this lesson is not to teach everything about Internet safety but to concentrate on two specific areas: 1) keeping personal information private, and 2) realizing that there is no way to really know who is communicating with you on the Internet. The specific learning goals are:

- Children and young people can learn when to give personal information to an adult and when to keep it private.
- Children and young people should never give private information to someone they don't know or can't see, such as people who might contact them through the Internet.
- **Parent Notice:** Send out a letter to the parents and guardians outlining the goals and objectives of this lesson. Let parents and guardians know that the lessons this year will concentrate on age appropriate Internet safety. For this age group, it will focus on keeping personal information private. It will also reinforce the need for children and young people to follow their parent's rules, particularly those about sharing personal information such as address, phone number, name, names of family members, and information about members of the family, their activities, etc.

Parents and guardians are the primary educators of their own children. This right of adults to educate their children, particularly in the area of morals, values, and human sexuality, is also recognized by the Church as "an educational duty."¹ The *Teaching Touching Safety* program establish guidelines and principles to assist parents and guardians in the sometimes daunting task of protecting children and young people from Internet predators. The program was developed to help educators, catechists, youth ministers, and other caring adults support parents and guardians as they provide their children and young people with education in this critical area. Many parents readily admit that their knowledge of Internet activity is inferior to that of their children and young people. In most public schools, even the youngest children are often given time during the week to work on the computer and become familiar with cyber activity. Lesson 7 is specifically designed to help parents and caring adults keep children and young people safe while they are working on the computer and "surfing the net" regardless of their age.

Dealing with the pre-adolescent age-key concept is "transition"

The junior high school child is experiencing a period of rapid growth. The emergence of interest in the opposite sex is occurring. These young people are concerned about physical change, body size, skin, and hair length. Concepts depend a great deal on body image as young people complain of being either too physically mature or too physically immature. Peer groups play an import role in shaping attitudes and interests. Caregivers need to regularly assure youngsters that changes are normal though the rate varies from person to person.

Parents, catechists, teachers, youth ministers, and other caring adults must also listen to children and observe what's going on in their lives. Let young people be themselves. Let them explore their self-expression but know who they are with, what they are doing, and

¹ Declaration on Christian Education, Gravissimum educationis, Proclaimed by Pope Paul VI, October 28. 1965, Article 3 at 44.

remind them of the importance of protecting themselves during this time in their lives. During this time, children are completely selfabsorbed and many are naturally less communicative.

Vocabulary words:

- Internet—Global communication network allowing computers worldwide to connect and exchange information.
- Social network—A site or place on the Internet where a number of users can communicate with each other in real time.
- Private—Personal information not publicly expressed.
- Rules—A principle or regulation that governs actions, conduct, and arrangements.

Supplemental Resource Material for Teachers

The complete grooming process employed by a child molester is usually three-pronged and involves physical as well as psychological behaviors. In person, the process may take months, even years to accomplish with regular face-to-face contact. However, through the Internet, predators can break down the child's defenses in a very short amount of time, particularly if the child is vulnerable or ignorant about the risks of the Internet.

The three aspects of the typical grooming process are *physical grooming, psychological grooming, and community grooming*—and all three can occur at the same time.

In the case of Internet seduction, the physical grooming becomes part of the process much later in the game. In fact, by the time the molester has an opportunity to touch the child it may be too late to protect the child from harm. There is no "build up" in the levels of intimacy of touch when the Internet is the initial contact point. Children solicited through the Internet are often abducted by the molester when a face-to-face meeting is arranged or there is any kind of physical contact. On the Internet, the physical grooming and community grooming are left out of the initial process, and the psychological grooming has some new twists.

The most important aspect of grooming through Internet contact is the *psychological grooming*. The molester establishes a relationship online by pretending to be someone in the child's age group. Through conversations about things the child is interested in, the molester will lure the child into social networks and, eventually is often able to convince the child to defy parents, grandparents, and/or guardians and meet the molester outside the home. The child is convinced that the molester is trustworthy and believes this person is a friend, someone that really likes and understands the child. The child may be convinced the online friend is the same age and has the same issues. Molesters know it is important to talk to children and young people on their level. They communicate in a way that children and young people understand and convince the young people that they are someone who can be trusted —someone just like them. On the Internet, this psychological grooming is particularly effective because none of the natural barriers of distrust or apprehension that might arise for a child are present. The physical appearance and real age of the molester are hidden from the child's view. The Internet provides a wall for the molester to hide behind and the child can't see the molester or the wall. Children and young people are particularly vulnerable to this approach because of their natural tendency to trust others.

Threats about not telling or threats about harming someone or something the child loves are not needed in this situation. The child's resistance is broken down through the communication process. Remember, the child often thinks that he or she is talking with another child. There is really nothing to tell mom and dad. After all, they are older. They would not really understand. Sometimes the child is conflicted but most of the time, unfortunately, what really happens is that the child bonds more to the molester.

On the Internet, there is no grooming of the community. In fact, the intention of the molester is to bypass the community altogether. In online seduction, the molester wants to remain hidden from view. He or she will create a relationship with the child that goes around parents, grandparents, and/or guardians and encourages the child to keep the conversations secret. This works because the child thinks the person on the other end of the communication is telling the truth.

The behavioral warning signs of a potential predator are evident in online communications but they are much more difficult for adults to identify. There is a barrier between the parents or caring adults and the predator that distorts everything about the relationship. That is why it is so important for parents and caring adults to be aware of the communications their children and young people are engaged in on the Internet and look for the signs that something is off.

Among the ways that behavioral warning signs show up in new and different ways because of Internet seduction are:

 Always wants to be alone with children. On the Internet, the predator has one-on-one access to children and young people through email and social networks. Email communications, though, are more risky. Parents can read email on the computer. Social networks are places for private, real time conversations that are more difficult and sometimes impossible to recover and read. Predators will invite children and young people to join them in social networks for "private" conversations.

- 2. Give gifts to children, often without permission. In person or on the Internet, predators find ways to give gifts to children and young people and tell them to keep it secret. The gift may be as simple as candy that parents won't allow. However, gifts are often more than that, particularly when they come from someone who made contact with the child over the Internet. In that case, the gift is likely to be entirely inappropriate—gifts such as perfume, flowers, lingerie, or expensive items.
- 3. Allows a child to engage in activities that parents would not allow. When meeting with children and young people online, predators lure them into online social networks and encourage secrecy. This activity is extremely effective at driving a wedge between the child and his/her parent(s). Child molesters look for children that are alone after school. They prefer to contact the young people between the time school is out and the time parents come home from work. This is another factor that convinces children and young people that the person "talking" to them is someone their own age. Why else would he or she be home and able to chat or email after school?
- 4. Uses sexually explicit language and tells dirty jokes. If parents and caring adults are monitoring young people's communications online, they can often see that this is happening and intervene. If, as is often the case, children and young people are allowed on the Internet unsupervised, it is possible for knowledgeable parents to recover this information but it may not be discovered early enough to protect a child from harm.

Knowing the warning signs means little where the Internet is concerned if parents are not monitoring their children's Internet activities. Find out where they are going on the Internet. Read email messages. Check out their social network. Put limits and filters on any computer children and young people can use and check regularly to make sure that filters are in place and working.

Generally, the grooming process is complex. On the Internet, it is even more difficult to identify and interrupt. This lesson is designed to focus on two things that children and young people can do to protect themselves from predators on the Internet. Two simple rules that can be the difference between safety and danger for children are: 1) keeping personal information private and 2) children need to follow their parent's rules in order to stay safe. Concentrating on these two rules will reinforce the message from parents and others about Internet dangers while keeping the benefits of the Internet available for everyone to enjoy.

Special Teacher Preparation Tool

Apply Internet safety rules in your own home, school, or organization. Read the attached VIRTUS® articles on the subject:

- Technology Safety
- Exposing the Dangers of Internet Chat Rooms

Technology Safety

"My mom and dad know absolutely nothing about computers; they don't even use them where they work. I got a computer for my birthday and right away I began meeting lots of cool people online. Right after school is the best time to chat online with my friends because my mom and dad aren't home and I have absolute privacy. Unfortunately, I have had some bad experiences online. I never knew that you could meet really gross people on the computer, but I don't let that stop me from chatting with other people. I spend a lot of my time online; sometimes I wish that we'd never bought that computer."

This scenario can be an all-too-common experience for young people today. Cyber technology and the Internet offer youth an incredible world of experience. With just the click of a mouse a young person can easily research a subject for school, chat with friends, check messages, or download a song. The electronic world can be fun and educational; unfortunately, like the real world, cyber technology, electronic communication, and the Internet also have inherent dangers.

Just as we encourage children and teens to behave in certain ways when dealing with strangers or even interacting with friends, we also need to teach them how to act safely and appropriately when online or while utilizing electronic communication devices.

Unfortunately the technology gap between adults and young people is widening. Children today have grown up with computers and they think of today's technology and the many associated devices as safe and a lot of fun. Many adults, on the other hand, view computers only as work tools and don't consider this form of technology to be a source of entertainment or as a constructive way to spend time away from work. However, the best way for adults to span the technology gap is to learn to use media and communication devices as their children do. This means one should try to chat with someone while using the computer online, use an online search engine to find particular information, download some music, or send a text message on a cell phone.

Youth of today need technology-conscious adults—trusted adult with whom they have open lines of communication—to teach them how to make smart choices about whom and what they will find when visiting the Internet. Simply communicating with kids may actually

be the best weapon against the child sexual predators that frequently use the Internet to identify potential victims. Sit down with your son, daughter, or a student and ask him or her to take you on a tour of the Internet and the electronic communication world they know.

Parents and schools need to be more actively involved with young people's computer and electronic communication usage than many probably are. Unfortunately, some parents will purchase a computer, set up Internet access, and then just walk away. If one is going to have a computer with online access in the house or at a school, children need to be educated by responsible and caring adults about the many dangers. A computer with online access can be just as dangerous as a car being driven by a teen without a license. Parents should regularly ask their children about their online activity and discuss the many new types of Internet activity popular with young people. Remember, no child-safety filtering software is perfect. Young people must be taught by responsible, concerned adults to be cyber-savvy.

Teenagers who use the various online services often feel that they don't need the same controls or restrictions as younger children. Unfortunately, teens are more likely to get in trouble while online than are younger children. Online social networks provide teenagers the opportunity to easily reach out beyond their parents, their circle of friends, or even their own peer group. Teens are frequently unaware that social networks are often the most dangerous online location a person can visit.

Law enforcement in the United States observed that child molesters' use of computers and the Internet exploded in 1997. No longer did the child molester have to assume a child-related profession or lurk in parks and malls to gain access to children. A molester could now sit at a computer and roam online from chat room to chat room trolling for children and teens susceptible to victimization.

It is vital to be aware of and familiar with new and changing technology and to maintain open lines of communication with children and teens. Young people might not be receptive to the message of safety if they feel that they are more knowledgeable about certain technology issues than are the trusted adults in their lives. Also, young people can be great teachers, so it is important to let them show *you* the sites they are visiting online, whom they are talking to, and what they are doing in today's world of technology. Remember, by routinely talking with young people, setting time limits, having them take breaks from online activity, and continually educating ourselves about ever-changing technology, we are all aiding in the guidance and protection of God's children.

Exposing the Dangers of Internet Chat Rooms

When visiting a chat room, it is not uncommon for a teen to become "friends" with one or more of the room's participants. Some of these online relationships are safe and can even be fun. Unfortunately, some relationships can turn out to be extremely dangerous. In these relationships a trusting teen may not realize that a "friend" is actuality lying about a multitude of things.

Dangers

Law enforcement has found that child molesters use chat rooms to gain easy and safe access to teens. For instance a 13-year-old girl can innocently join a chat room with the name "13 Single and Looking." The girl would think that because the name of the chat room describes her own situation she would be able to meet other unattached teens in her own age group. Unfortunately, child molesters will gravitate to a chat room with this type of name looking for the opportunity to meet, converse with, and then sexually exploit children. In many situations a child molester will assume the identity of a young man. During a chat or during the course of several chats he will appear to act very concerned and understanding, and in some cases will offer the girl compassionate advice. Because of the caring and the seductive talent of child molesters, teenagers should be warned that when they are in a chat room, they should <u>never</u> provide anyone with private information, personal information, and especially their specific physical location.

During a chat a significant danger occurs when the molester encourages a teen to meet him or her in person so they can "talk about" his or her concerns "in person." Any teenager who visits chat rooms should be warned to <u>never</u> physically meet with anyone they have talked with online unless he or she first discusses the meeting with his or her parents or with some other responsible adult.

In the hundreds of arrests of online sexual predators that our unit conducted in Chicago, we found that in almost every case the offender had previously met and sexually abused one or more teenagers in locations across the United States and in Europe. In most of the cases of sexual abuse that we identified, none of the children had reported the sexual abuse to their parents or to law enforcement.

Some services or even some websites offer "private chat" areas. Teens may utilize these private areas to talk with friends away from the prying eyes of others. Some of these chats may be truly private, while others may be listed with the names of the chat rooms on a directory. If the chat room name is listed on a directory, nothing will stop a stranger from entering the chat room.

Junior High Level, Grades 6, 7, 8 (ages 11 to 14 years)

During some chats, a "friend" may offer to upload a photo. This can be dangerous because the upload may contain a virus, a Trojan horse, or Spyware. This software can then be used by a molester to view the teen's computer—keystroke by keystroke—or with some Trojan horses to actually take control of the teen's computer. In other cases a molester may upload pornography or child pornography as a way of soliciting a reaction from the teen. A simple safety rule is to never accept an upload from anybody in a chat room.

Screen name

The screen name is the name or the identifier by which thousands of people will identify the user in the chat room. A screen name is also known as a username, nickname, or screen ID. The screen name for an online service is frequently associated with a connection password. Most online providers allow you to use multiple screen names although the passwords are registered with the service. The Internet Relay Chat (IRC), that I discussed in the January 31, 2005, VIRTUS *Online* article, allows the user to change his or her password every time that that person enters a chat room or multiple times during a single "chat." The names are not registered in the IRC.

Frequently a teen will attempt to pick something unique as a screen name so that it can be easily recognized by other teens such as "bobbi13" or "hoodsy14." This can be dangerous as a molester can easily identify this user as being a teen. A screen name should never have a child's real name, age, or anything else that might identify the online user as a teen.

Profile

A profile is the location where an online user can "publicly" list his or her personal information and special interests. Because this information is posted and is open to the public, anyone can view it. Unfortunately, a child molester can easily do a word search of the profile information to locate children or teens living in his or her own city or even in his or her own neighborhood. Once a local teen has been located, the molester can easily determine when the teen is online. He can then engage the teen in a chat conversation, while using the information from the teen's profile as a catalyst in the conversation.

For safety purposes, a child's profile should never include:

- A photograph of the teen.
- The first name, the last name, or any other name the teen may use.
- The teen's home address, city, or state.
- Home or mobile telephone numbers.
- Social Security Number.
- The name of the teen's school.
- The name of the school's sports team or the school colors.
- The names of any friends.

In addition to never providing personal information in a profile, teens should be warned that for their own personal safety they should never share any of this information with the participants of any chat room or while using an Instant Messaging system.

Instant Messaging (IM)

Known by several other names, Instant Messaging is used by many teens as an alternative to waiting for a response to an email message. With this software, it allows teens to send and receive private—and in some situations unsolicited—messages from other online users. AOL users utilize Instant Messaging as a form of private one-on-one communication. Other online services may use software called Instant Messenger, which makes it possible to exchange messages with one person or with several people at once.

Protection

When chatting online teenagers may become uncomfortable as the result of being harassed, bullied, or subjected to obscene language. They can also be stalked or solicited for sex. Some online services such as America on Line (AOL) offer safety controls connected with their chat rooms. Most of these controls are of the "on or off" type. This means that a parent is prompted with a question and then asked to check yes or no. An example of this type of questions is: "Do you want your child to receive email?" Or, "Do you want your child to access the Internet?" The problem with these controls is that some children will find a way to circumvent the parental controls. Because many of the controls are easy to manage, a determined, creative, and "techie" teen will find a way to circumvent them.

Unlike some of the online services that provide parental controls, the Internet Relay Chat (IRC) has absolutely no built-in parental controls or safety mechanisms.

Conclusion

Chat rooms can be a source of amusement, but chat rooms can also be very risky. Prior to a teen or a child joining in the fun of online chatting, a frank discussion should occur where the dangers of online chatting are discussed and specific rules are established to help protect the child from online predators.

Junior High Level, Grades 6, 7, 8 (ages 11 to 14 years)

Lesson 7: Internet Safety

Keeping Personal Information Private

Educators, catechist, youth ministers, and other caring adults should prepare by reviewing the entire lesson plan <u>and</u> by reading *Teaching Touching Safety: A Guide for Parents, Guardians, and other Caring Adults.* During the class, follow the instructions to complete as many of the activities as possible in your allotted amount of time.

- Activity #1: Play the introductory DVD to begin the lesson.
- Activity #2: Lead the discussion on private information with children in the class.
- Activity #3: Discussion regarding Internet Safety Rules.
- **Prayer:** A suggested prayer is provided at the end of the lesson. If you wish, you may use this prayer to conclude this lesson with your students.

Supplies and Preparation:

Opening DVD DVD Player and TV

Activity #2—Classroom Discussion:

Project instructions:

[Separate poster display boards with the Definitions of "Internet" and "Private" on them]

- Do you ever think about the number of words we use that we really don't know what they mean or could not define?
- For example, we talk about the "world wide web" or the "Internet" but what is that? [NOTE TO TEACHER: Have them say how they would define these two terms. After you have heard from some of the students, share the definition from the dictionary or have the students look them up in the dictionary.]
- One dictionary defines "Internet" as: a vast computer network linking smaller computer networks worldwide.
- When you know the definition, it helps you understand what people are saying and, sometimes, how the system works. Just thinking about the definition of Internet can help us create a picture in our mind and helps us see something we can't see—the Internet.
- Some people call the Internet the "information superhighway." In some ways it is similar to a highway and in other ways it is very, very different. What are some ways a highway or freeway is similar to the Internet? [Have them shout out answers. Similarities will include the ability to travel quickly from one place to another. The fact that you don't have to travel alone. There are stops along the way and every one of them has a sign that tells you the name of the spot. You can see where you are, but you can't see what's ahead on the Internet or the road.]
- In what ways is a highway different from a highway or freeway? [Be sure that they realize that there are lots of signs on the road that let you know about danger ahead or warn you of potentially risky situations. These signs let you know what to notice and watch out for. There are no signs on the Internet, so you never really know if there is danger or risk where you are or where the Internet takes you.]
- If the Internet is a superhighway, it is also a super secret highway. The Internet will take you to amazing places, but you have no idea how you got there or who is traveling with you. Let's think about how we use the computer and the Internet.

- How many of you have the ability to use the computer at school? (raised hands) at home? (raised hands) at the library? (raised hands) Where else do you use the computer? [Have the students share other access points they have for Internet and computer use.]
- Where else do you have access to computers? [NOTE TO TEACHER: This is an opportunity to listen for the many access points that children have available to them. When discussing Internet safety issues, remember to include any other venue for computer use that the young people mention in this section. Also, be careful not to make it seem wrong for using the computer somewhere other than at home with adult supervision. You want to hear their thoughts, and making them feel guilty at this point will simply shut down the conversation.]
- What do you use the computers for? [Again, listen for the various ways students use their computer access so that you can use them in the discussion. It is not necessary for you to know everything about these different types of communication but you should at least know the following:
 - Email—a system for sending messages via telecommunication links from one individual to another using computers or terminals.
 - **Chat Room**—a site on the Internet where several people can have an online conversation in real time. It is a computerized version of a face-to-face conversation except it is online and the real identities of all involved are hidden from view.
 - Social Network services—are not to be confused with "social networks." Social network is a key concept in modern social sciences such as sociology and anthropology. Social networks are basically maps of the relationships within organizations and between individuals based on such things as visions, values, etc. A social network service is an entirely Internet based phenomenon. It focuses on building <u>online communities</u> of people that appear to share interests and activities, or are interested in exploring the interests and activities of others. Social networks for purposes of this discussion are <u>web based</u> and provide a variety of ways for users to interact, including <u>e-mail</u> and <u>instant messaging</u>.
 - Instant Messaging—known by several names, allows users to send and receive private—and in some situations unsolicited—messages from other online users. AOL users utilize Instant Messaging as a form of private one-on-one communication. Other online services may use software called Instant Messenger, which makes it possible to exchange messages with one person or with several people at once.

These communication tools, unique to the computer and the Internet, come complete with high risks of abuse by sex offenders. This discussion is designed to start to help children see the risks that are hiding behind a computer screen.]

- Another word we use a lot but rarely think about its definition is "private." The dictionary defines the word private as: Personal information not publicly expressed.
- What are some examples of the type of personal information about you that is private—things you would not share with just anyone you meet or see on the street? For example, your address and phone number are illustrations of private information that you might give to someone in person who needed to know, such as a teacher or classmate. However, this is private information that no one should give out on the Internet. What are some other examples of private information that should be kept private when we are on the Internet? [Note: Let the children discuss the type of information that should be protected on the Internet.]
- When we put the Internet and private information together, something potentially dangerous happens.
- What is the risk of giving out private information on the Internet? [Listen for what they think are the risks or whether they are aware of any risk.]
- The biggest risk of sharing any private information on the Internet is that you never really know who you are talking to. Remember the Internet is a super highway that no one can see and there is no way to find out if people are being truthful. They can and often do say anything they want on the Internet trying to convince you that they are trustworthy in order to get you to give out your private information. The problem is you have no way of knowing who is really at the other end of the conversation. Also, once you put information on the Internet, there is no real way to get it back...you can't "untell" a secret.
- It is sometimes difficult to remember that the people you chat with on the Internet could be lying to you about their age, their name, their interests—everything. The conversations seem so real. But people on the Internet are hiding behind a computer screen. Even if they are telling the truth. Even if the person you are "chatting" with is a 10 year old going through the things you are dealing with, there is no way for you to be sure about that—you don't know whether there is really a 10 year old at the other end of your communication—so, private information needs to remain private unless we know who is getting it and why they want it.

Activity #3: Internet Safety Rules

Consider the following statistics and/or reference recent news headlines:

Some 57 percent of parents worry that strangers will contact their children online. These worries are well grounded. Close to 60 percent of teens have received an instant message or email from a stranger and 50 percent report emailing or instant messaging with someone they have not met before. (*Pew Internet & American Life, "Teenage Life Online," June 20, 2001*)

65 percent of parents and 64 percent of teens say that teenagers do things online that they wouldn't want their parents to know about. (Pew Internet and American Life, "Protecting Teens Online," March 17, 2005.)

Assist your class in developing a list of Internet safety rules that they agree to follow as well as share with their parents. Because creating a sense of ownership and empowerment to do the right thing is important, make this a student-led process. Consider making these rules an ongoing part of the class' culture, referring to and implementing them as often as possible.

Also, consider making periodic assignments or designing class projects around the themes of accountability and technology issues. Current events and news headlines regularly provide timely and relevant starting points for such studies.

Junior High Level, Grades 6, 7, 8 (ages 11 to 14 years)

Prayer to end the lesson:

[Remember that this is a variation of an Old Catholic Traveler's Prayer to be said before beginning the journey. Remind the students that, as they grow up, they are on a kind of journey through life. Each time they leave their home or their room to go out on their own, they are traveling. Prayer can help prepare them for the journey and guide them along the way.]

My holy Angel Guardian, Ask the Lord to bless the journey that I undertake, That it may benefit the health of my soul and body; That I may reach its end, And that, returning safe and sound, I may find my family in good health. Guard, guide and preserve us throughout the day and night.

Amen.