



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

High School Level, Grades 9 through 12 (ages 15 through 18 years)

Lesson Plan 7: Internet Safety Preserving Anonymity on the Internet

### **Getting started with Lesson 7:**

**Principle:** Educating children about Internet Safety. Specifically:

1) Some Do's and Don'ts of interacting with people on the Internet, and

2) 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 talking 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." 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.

<sup>-</sup>

<sup>&</sup>lt;sup>1</sup> Declaration on Christian Education, Gravissimum educationis, Proclaimed by Pope Paul VI, October 28. 1965, Article 3 at 44.

High School Level, Grades 9 through 12 (ages 15 through 18 years)

### Dealing with the teens—key concept is "searching"

This is the age where all the experiences began with puberty—the physical changes and the developing emotions. The self-consciousness deepens and matures. The world of "children" is now renounced. Teens believe in their immortality and may tend to be reckless in behavior. Although it may appear that they reject authority while defining their own independence. In reality, they rely on the strength and support they find in parents and meaningful adults

### 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:

1. 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

High School Level, Grades 9 through 12 (ages 15 through 18 years)

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.

High School Level, Grades 9 through 12 (ages 15 through 18 years)

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 never 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.

High School Level, Grades 9 through 12 (ages 15 through 18 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.

High School Level, Grades 9 through 12 (ages 15 through 18 years)

#### **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.

High School Level, Grades 9 through 12 (ages 15 through 18 years)

High School Level, Grades 9 through 12 (ages 15 through 18 years)

Lesson Plan 7: Internet Safety – Preserving Anonymity on the Internet

## **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 (optional).

**Activity #2:** Lead the discussion on private information with children in the class.

Activity #3: Discussion questions.

**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

Print picture of highways and superhighways.

## Activity #2—Classroom Discussion: Protecting Private Information and Preserving Anonymity on the Internet

## **Project instructions:**

**Supplies:** Poster displaying screen names

- Before the Internet it was fairly easy to protect your personal information from being stolen or used by someone
  other than yourself. There are new crimes being committed every day that no one ever thought of until the
  "Information Super Highway" was invented and became a normal part of our every day life.
- Given the part the Internet plays in our daily life, it is hard for us to imagine life without it. What are some of the ways we use the Internet in our daily lives?
  - o Research
  - Communication
  - Education
  - o Banking
  - Shopping
  - Downloading music, movies, books
  - Meeting people
  - Sharing information

[Students may give specific examples of ways they use the Internet. Use the examples to demonstrate these and other uses of the Internet. The important thing for this lesson is to really have an experience of how pervasive the Internet is in our lives. The many, many uses for the Internet and the many ways it is part of our lives can make it seem harmless and friendly. This realization is key to the students finding value in the material that we intend to share in the lesson.]

- Most of the ways the Internet impacts our life are valuable, safe, and productive. However, one of the risks of so
  much positive involvement with the Internet is that we can begin to think about the Internet as a safe place to be.
  There are millions of sites to visit and an almost unlimited number of things to do on the Internet and, at the
  same time, there are a number of ways that others can take advantage of us on the Internet.
- What are some risky or even dangerous things that can happen on the Internet?
  - Identity theft
  - Scams—Example, email from Nigeria asking for help to move money from the country for a small fee that will, in return, get the receiver a big share of the money being moved. There is no money to move. The email is just trying to get the fee forwarded to the scam artist.

High School Level, Grades 9 through 12 (ages 15 through 18 years)

- Cyber bullying—Cruel, threatening, or bullying messages that show up in your email or through chats online, social network sites, or through instant messaging. The messages can be annoying and, sometimes frightening. The messages may come from former friends or others that you know or people that know you.
- o **Predators**—People that attempt to lure you into a situation where they can take advantage of you.
- Hackers—People that access your computer without your permission. They can gather information off your
  computer without you knowing they are there. They use the information for a number of purposes including spam
  and identity theft.
- One of the reasons for the risks and dangers of the Internet is that it is very hard to be sure who we are really talking to. Screen names don't really tell us the truth about people. For example, let's look at some screen names and see if we can tell who they are and whether that person is safe. [The following are from news stories. The screen names were discovered and reported for others to recognize. The opportunity is to show the screen name on a flash card or write it on a display board and then ask the students what they might say about the person from seeing the name. Then after they consider their own interpretations, tell them who the person really turned out to be. Some are "bad screen names" and some are not.]
  - "singindiva"—this screen name is used both by a 64 year old grandmother that is known for her singing ability and a middle school music teacher from the Midwest.
  - "rcdunlap1971"—this turned out to be a 36 year old man named Robert Dunlap with two kids. He was arrested
    for sending videos of himself naked to someone he thought was a 13 year old girl. (The Source of this is
    <a href="http://www.badscreennames.com/">http://www.badscreennames.com/</a>. This is a website dedicated to identifying bad screen names and making them
    public to help keep children and others safe.)
  - "tuttyirish"—a single adult female in her 40s who is Irish descent but was born, raised, and now has moved back to in Montana
  - o "fanfest2004"—a 30 year old child molester
  - o "clintbo2001"—a 30+ year old pedophile that targets teenage girls online
- As you can see, a screen name rarely tells you enough to guarantee that you are talking to the person you think is on the other end of the communication. Who will share their screen name and why they chose it? [This is a good time to share your screen name and why you selected it. If the students are not volunteering, ask some of them about their screen names. If there is a large group, you might put them in groups of four or five and have each share what they use or have seen related to screen names. The point of this discussion is for the students to begin to recognize that screen names are not really much different than a character name in a book of fiction or a play. They are not the real person and we never know what is really behind the name or why someone would use it. Perhaps it is for fun and perhaps not. There is just no way to tell so we should never rely on what someone calls himself or herself online, or what they say about themselves online as the truth.]
- In order to take advantage of the benefits of the Internet and avoid as many risks and dangers as possible, we
  need to realize the risks involved and take the steps necessary to stay safe and protect ourselves and our
  families from harm.
- The easiest way to do that is to create and honor at least the following two standards for material or information online.
  - Never give out any private or identifying information on the Internet to anyone whose identity you cannot verify or without your parents' permission.
  - Never post anything on a website or web space that would or could be an embarrassment to you if it was seen by a college recruiter, a potential boss, or anyone that you might want to make sure is left with a good opinion of you. [There are instances of people making silly mistakes by posting something on the Internet that then came back to haunt them. For example, an article by Randall Stross in the New York Times entitled "How To Lose Your Job on Your Own Time," shares about the growing trend of employees losing their jobs based on inappropriate or unprofessional online content. The author points out that the nature of the Internet gives off-theclock activities more visibility and employers are interested in what workers post online. There is no legal recourse to employees that find themselves in this situation. With the lack of legal recourse available to workers, poorly-chosen words or photos posted online can lead to termination. A female teacher in a Pennsylvania High School lost her teaching credentials and as well as her teaching position when administrators found her social network site's profile photo. The photo was not taken on school grounds and was shot after work hours. In it the woman is wearing a pirate hat and holding a plastic cup. The picture is labeled "drunken pirate" and school officials said that merely posting the photo online was a breach of professional standards and promoted underage drinking. Another example of the cost of this kind of lack of forethought is a situation that occurred in late 2008. A 25 year old college student working on completing a degree in Criminal Justice is running for Police Chief in his community. Five years earlier he dressed as a wrestler and made a YouTube video about drinking and raising the drinking age—as he was drinking beer on camera and not yet 21. Now, as he campaigns, more people are paying attention to the Internet video than what he has to say as a legitimate, serious candidate for

High School Level, Grades 9 through 12 (ages 15 through 18 years)

the job, and it is costing him a great deal. He just never thought about the long term consequences of this action when he did the video. The point of this discussion is to encourage the students to look to the future and how this might look to someone they really want to impress if it were to come up at an inopportune time—because it will. Once it is on the Internet it will not go away.]

- Eliminating or protecting private information from the Internet begins with identifying the kind of information that should remain private. If you considered that the "Private" information we are talking about is the kind of information that could help the other person find you, what kind of things should you protect on the Internet.
  - o [Invite students to make a list of the kinds of private information that should be protected in their communications on the Internet. This is an opportunity for them to start to realize how much attention they need to pay to their communications if they are going to stay safe and still enjoy the opportunity of communicating with others through cyberspace.]
  - Make the following points:
    - Name
    - Address
    - Parents names
    - School you attend
    - City where you live (particularly if it is a small town or community)
    - Where you or your parents work
    - Names of best friends
    - Name of parks or landmarks in your neighborhood
    - Grandparents names and/or addresses
    - Any information that would tell someone where you are or will be at a particular time, such as the name of your favorite hang out or the church you attend
- How difficult do you think it is to keep private information private online?
- Let's just look at some possible communications and how you could respond to make sure that the communication maintains a safe environment for you. [Ask students to quickly write potential responses to possible email messages or IMs—in the same sort of timeframe that they would normally respond online to an IM or an email. Make sure that the communication protects identity and private information. Give them only about a minute to answer the email or IM.]
- Now let's look at each of the communications and hear how you responded. [Go through the communications one at a time and let the students that responded to each communication share their response. As they do, ask the other students if there is anything in the communication that would help them locate the person or find out where they live, work, go to school, or attend church. Then do the exercise again and ask them to take a little more time and think through their response and read it carefully before they hit "send" for an IM or email.
- We recommend that you stay out of social networks until you have become very, very good at communicating
  quickly without revealing any private information that could place you or others at risk or in danger. Remember
  that no matter how safe or good your intentions are or how much the person online seems to be sympathetic to
  your situation, you do not know who it is at the other end of the communication and you do not know what is his
  or her intention.
- You have a great deal of freedom on the Internet. That freedom comes with a great deal of responsibility. When you learn to drive a car, you learn the rules of the road, and you know that the rules are to protect yourself and others—you must follow the traffic rules. Sometimes you don't and often, when you ignore the rules you may get hurt, or it costs you or perhaps you and others something. The rules of the road are there to promote a safe and valuable experience of driving and to make sure that the shared experience of everyone on the road is fun, safe, and positive. Following these two rules of the Internet—keeping private information private and making sure that nothing you post will ever embarrass you or be used against you— is how we can make sure that the shared experience of the Internet is safe, fun, and positive for everyone involved.

High School Level, Grades 9 through 12 (ages 15 through 18 years)

**Activity #3: Discussion Questions:** Teachers lead a group discussion based upon the following statistics and discussion questions. Guide the discussion with responses based upon material from the lesson. Encourage open communication by emphasizing to students that this exercise is to generate awareness and discussion about Internet usage and safety issues—*not* to get anyone in trouble.

Over 85 percent of U.S. teens ages 12 to 17 currently use the Internet—this represents about 21 million young people. (Pew Internet and American Life, "Teens and Technology," July 27, 2005.)

Related Group Discussion Questions:

- 1. How many of you use the Internet?
- 2. How many of you use the Internet everyday (either on a computer or phone)?
- 3. Why do you use the Internet?
- 4. How do you think that your Internet usage affects the quality of your life (both positively and negatively)?

**52** percent of online teens say they do not worry at all about being contacted online. (Pew Internet & American Life, "Teenage Life Online," June 20, 2001)

Related Group Discussion Questions:

- 1. How many of you are concerned about being contacted in person by someone you do not know—what is this stranger came to your house to contact you or was waiting for you in the parking lot this afternoon? How would you feel about it? What would you do?
- 2. How many of you are concerned about being contacted online by someone you don't have any real information about? How would you feel about it? What would you do?
- 3. What is the difference?

30 percent of teenage girls polled by the Girl Scout Research Institute said they had been sexually harassed online. Only seven percent, however, told their mothers or fathers about the harassment, as they were worried that their parents would ban them from going online. (Girl Scout Research Institute 2002)

Related Group Discussion Questions:

- 1. How many of you have ever had what you think of as a negative experience online?
- 2. What do you think is the difference between being bullied or harassed online and in person?
- 3. What factors might prevent a young person from telling their parents about such an event?

27 percent of teens said that they have known a friend to actually meet someone whom they only knew online. (Teen Research Unlimited, "Topline Findings from Omnibuss Research," October 2005.)

Related Group Discussion Questions:

1. What advice would you give a friend who was planning to physically meet someone he or she only knew through online contact?

Online teens admit that they frequently communicate with people they have never met: 54 percent have Instant Messaged a stranger, 50 percent have emailed a stranger, and 45 percent have participated in a chat room discussion with a stranger. (Teen Research Unlimited, "Topline Findings from Omnibuss Research," October 2005.)

Related Group Discussion Questions:

- 1. What do you consider to be the definition of a "stranger?"
- 2. Does your definition of a stranger change when dealing with online contacts?
- 3. Let's develop a definition of the idea of a "stranger" that is applicable to all situations...

High School Level, Grades 9 through 12 (ages 15 through 18 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.