Internet Safety Toolkit







Table of Contents

- Introduction
- 4 What can we do?
- **7** Help with uncomfortable conversations
- 8 How are children accessing the internet?
- Phone safety
- Sexting
- Sextortion
- Social networking
- Signs your child may be at risk
- Internet fraud
- Cyber-bullying
- True or False
- Did you know?
- Safety pledge
- Additional resources







Introduction

The Internet Safety Toolkit is a guide to help keep children safe.

The internet and other technologies have drastically changed the way children interact with their world; the internet has become a major part of nearly every aspect of our lives. Today's children have access to the internet at very young ages; they are comfortable with it and able to interact with it easily. While the internet is full of learning opportunities, it also allows access to inappropriate sites and a wide range of things that can place children at risk.

Social media, web based communication tools allowing people to interact by sharing information on a variety of platforms, has changed the way we communicate. Some of the more popular social media networking applications teens are using to communicate include Facebook, Twitter, Instagram, Snapchat, and KiK. While the sites themselves are not harmful, the atmosphere of perceived anonymity created by non-face-to-face communication can become dangerous to teens and youth; they are more likely to engage in risky behavior not normally considered in actual face-to-face situations.

The good news is children and adults can safely use technology and can avoid risks and respond effectively to unsafe situations, if armed with information and skills. Adults who recognize the risks will be better prepared to intervene and lessen the potential negative impacts.

This Toolkit, created in collaboration with experts from across the state of Kentucky, helps provide information needed to keep children safe.



What can you do?

Educate yourself. Take time to learn how to use technology, monitor usage and implement parental controls.

Understand the risks:

- False identities are easy to create
- Predators are real
- Not all information is private
- Kids have increased access to technology
- Things you read online may not be true

Utilize parental controls offered by service providers and/or blocking software. Providers can explain options and help you understand how they work.

Be aware the internet is accessible on home computers, phones, gaming devices, iPod touch, iPad, TV, etc. Do not allow internet usage to be a private matter. The internet can be accessed in many places with no supervision. Parents must know their children's usernames and passwords for all online accounts.

Model appropriate behavior. Many of us have made decisions we may need to rethink regarding our own internet usage, including:

- Posting of pictures
- Posting rants
- Sharing too much information
- Open, vulnerable profiles

Be familiar with laws regarding technology and transmission of sexual material by youth. Did you know, if a child takes a photo of him/herself naked, he/she could be guilty of producing pornography? Did you know if you find a photo of a naked child and you then show that photo to another adult (who is not law enforcement), you could be guilty of distribution of child pornography?

Have a plan in place so your children know what to do in the event something happens as a result of online activity. Both you and your children will respond more appropriately if there is a plan.





Communicate, communicate, communicate!

Do not rely solely on parental controls; while they are important tools, they will only alert you when something has gone wrong. The goal is to help your children make good choices; this involves a lot of communication.

- Talk to children about positive aspects of internet use, as well as the dangers.
- Have honest and open discussions about how child predators may go online to exploit or victimize youth.
- Discuss how children's actions can lead to victimization and irreversible consequences.
- Kids must realize things they see online may not be true and they may be communicating with someone who is not who they claim to be.

Spend time with your children online. Have them teach you about their favorite online activities and sites. Enjoy the positive aspects of the internet.

Learn about chatting and messaging. Understand chatting, instant messaging, texting and other technologies which allow for real time dialogue between two or more people. Parents must know how chatting and messaging works, when it is taking place and what measures can be taken to monitor the activity. There is a lingo associated with chat and texting that is meant to keep adults in the dark. Knowing the language will assist you as you monitor your child's activity. (See examples on page 10.)



Communicate early and often!

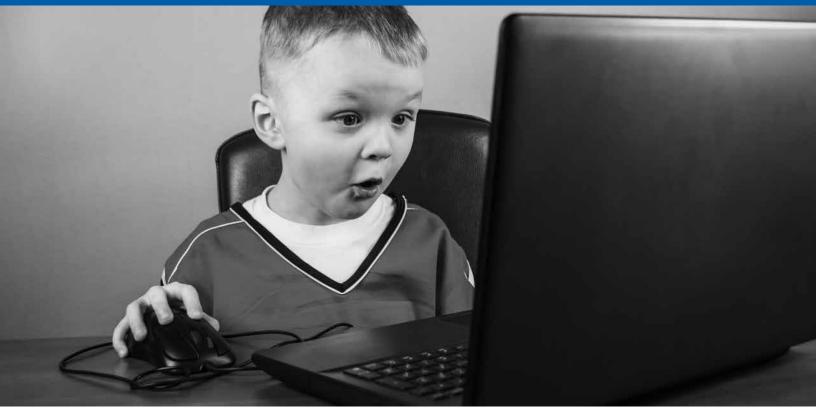
Review age appropriate online safety material found at **www.netsmartz411.org** with your children. Discuss issues on a regular basis starting at a young age. Don't wait for something to happen to have discussions.

Set guidelines with first use. By doing so, responsible behaviors and habits are established from the initial use of the internet.

Teach children about predator strategies such

as seducing their targets through the use of attention, affection, kindness and even gifts. Predators often invest considerable time and energy into finding and befriending victims. They may be familiar with the latest music, hobbies and interests of children. They know how to lower children's inhibitions by introducing sexual content into their conversations.





Limit the amount of time

your children are allowed to spend using technology. Online activity, like other "screen time" activities (television, video games, etc.) should be used in moderation. Keep track of how long your children engage in these activities.



Set limits and instruct your children to:

- Never post pictures online without permission and explain why this action may be dangerous.
- Never request or agree to a face-to-face meeting with someone they met online, even if a relationship has been established. Help your children understand why this may be dangerous.
- Never give out identifying information such as name, phone number, address or school name and explain why this is important.
- Never download pictures from an unknown source; this is used as a method to transmit sexually explicit images.

- Never respond to messages or bulletin board postings that are sexually suggestive, obscene or harassing in nature.
- Never use the internet in an aggressive manner to make fun of, ridicule or harass another person. Help your children understand why it is important for them to tell someone when this is happening.
- Establish family practice to limit unsupervised access to technology. For example, from day one, make it a rule cell phones are kept in a parents' room overnight.
- Do not download file-sharing programs (programs that share things such as music or pictures). Often times these files are illegal and can be utilized to distribute child pornography.

Take time to discuss each limit with your child. Help them understand the risks, and why the rule is meant to keep them safe.





Help with the uncomfortable conversations

Sometimes, it seems easier to run a marathon than to sit down and talk with your kids about uncomfortable topics such as safety on the internet. In a perfect world, you wouldn't need to have this conversation, however there are dangers your children must know about. Here are some suggestions to help you start those conversations.

• Begin with initial use of technology and use developmentally appropriate examples.

"Look at that horrible picture of mommy with messy hair on Facebook- I don't want anyone seeing that photo! We have to be careful about putting pictures online."

• Remember to lock the door.

"We lock doors so strangers can't come into our home. It is important to not allow people we only know online in our homes or private lives."

- Use rules and guidelines as safety tools, rather than punishment. Setting rules early sets clear limits that become acceptable habits; they will be better received if implemented early rather than as a result of a broken rule.
- Use "Self" examples.

"When I was in high school, I made some silly mistakes and had some embarrassing moments." Talk about what it would be like had those incidents been documented permanently online.

- Remember your own childhood. Being curious about sex is normal. The internet simply provides a new way to explore. Expect children to violate rules, it is normal. Be prepared to respond calmly, while maintaining open communication.
- Use current events to begin a conversation. "Did you see the news story about (insert title of recent adult situation)? Think about how the adults/spouse/parents/ children must feel. Talk about what the adult could have done differently.

• Be frank regarding lifetime consequences.

"I think it is important you know and understand how one action (such as sexting with a girl/boyfriend) can have life-long consequences. Do you understand sexting could result in a child pornography conviction and sex offender label? Think about how that would affect your life, your ability to get a job, to be a coach, to volunteer, etc."

• Have a plan.

Have a plan or agreement in place between parents and children to deal with issues that may be uncomfortable or unsafe (even if it was a broken rule that allowed or created the unsafe situation).



How are children accessing the internet?



Having grown up in a world where accessing the internet is a daily occurrence, children rely on a variety of devices in their everyday lives. According to a 2014 study by Edison Research (www.edisonresearch.com), cellphones were the top device owned by children and teen internet users. Internet-connected games consoles were common, with approximately seven out of ten individuals owning one. Children appear to be using the gaming consoles more to connect to the internet than for their original intended purpose of playing games. Children and teens also report using a tablet (55%) and internet-connected TV (44%) to access the internet at home.

Understanding the ways in which children and teens are accessing the internet gives us some insight into the different steps we may need to take to help our children be safe. When parents are considering monitoring internet usage as a safety measure, it is important to remember all the devices used for that purpose.

CADIZ, Ky. (3/4/16—According to a Kentucky State Police report, on Feb. 5, 2016 KSP was made aware of suspicious Internet activity regarding a Trigg County resident.

The report said the allegations stemmed from information obtained from the

National Center for Exploited and Missing Children in Washington, D.C. Upon receipt of the information, KSP Post 1 Internet Crime Against Children Detectives assigned to the ICAC Task Force began an investigation.



Phone Safety

Cell phone accessibility has made keeping in contact with kids easier than ever. This ability to immediately be in contact with children is convenient and reassuring. Long gone, however, are the days when parents were aware of every call coming into the home. Children now receive calls and messages without anyone knowing frequency or content. It is very important to teach youth how to appropriately and safely communicate using cell phones and other handheld devices.

- When purchasing a phone/plan, review phone options and parental controls.
- Both you and your child should become familiar with the phone and all features.
- Monitor cell phone usage via online management of the account or monthly phone bills. Opt for a detailed bill outlining each number receiving and sending calls and texts.
- Communicate with your child how talking on the phone can cause them to be distracted and less aware of his or her surroundings.
- Warn your child about the dangers of texting while driving. Set a good example.
- Limit internet access on cell phones.
- Consider deactivating the camera feature on your child's phone.
- Pay attention to your child's behavior as it relates to texting.

Sexting

Sexting is sending sexually explicit messages or photographs between mobile phones or other handheld devices; it is a common practice among youth. Many youth engage in this practice willingly; however, youth can also be coerced into sending a picture or sexually explicit text. Education is critical to prevent irreversible consequences. Sending and/or receiving sexually explicit pictures or texts can have consequences well beyond embarrassment and the potential for exploitation.

Youth need to understand the seriousness of sexting. Sending or receiving sexually explicit photos (even when it is a picture of themselves) has a multitude of consequences, including:

- Arrest for child pornography
- Suspension from school
- Loss of employment
- Humiliation
- Risk of harassment, bullying or threats (i.e. if the picture to be forwarded/shared with unintended recipients including classmates, parents, child pornographers)
- Suspension from athletic teams, clubs and/or extracurricular activities
- Risk of being identified as a sex offender for receiving or sending child pornography and inability to gain future employment





Texting Lingo Things a parent should know

9 - Parent Watching
99 - Parent Gone
53X - Sex
ADR - Address
CD9 - Code 9 - parents are around

KPC - Keeping Parents Clueless **LMIRL -** Let's Meet In Real Life **PIR -** Parent <u>In</u> Room **POS -** Parent <u>Over</u> Shoulder **RU/18 -** Are You Over 18?

Remember, youth may not have the developmental skills to anticipate the consequences of their actions. They will need caring adults to help them fully understand the risks. Action steps adults can take include:

- Purchasing and implementing parental controls
- Talking to your youth. Make sure they understand rules, consequences, and that this is a safety issue for them. It is your job to protect them from harm.
- Communicating openly about potential or actual victimization (including bullying, harassment, and threats)
- Reporting any suspected illegal interaction with adults to your local law enforcement agency or Kentucky State Police
- Taking the phone or limit access

Sextortion and Cyberstalking How a Single Tip Uncovered an International Scheme

04/26/16

The investigation that uncovered a far-reaching sextortion scheme by a U.S. State Department employee at the U.S. Embassy in London all started with a single complaint by a young victim in Kentucky. She went to the police...

and a statement of the

A former high school teacher in Johnson County has been sentenced to 14 years in prison after admitting he received nude photos from a female student and had sex with her.

Sextortion

Sextortion is a type of cybercrime that occurs when offenders use personal information – often images stolen from a computer or obtained by hacking into a webcam – to force victims to engage in some form of sexual activity. Offenders frequently target multiple victims, a majority of whom are children. They scare victims into providing sexually explicit images or videos by threatening to send information to their family or friends. In a recent study, 71% of the cases involved victims under the age of 18; social media was used in 91% of those cases.

Children tend to be trusting online and will befriend people even though they know very little about them. Offenders take advantage of this and target children. Sextortion is a crime. The coercion of a child by an adult to produce what is considered child pornography carries heavy penalties, which can include up to life sentences.



Social Networking

The popularity of social networking sites such as Facebook, Instagram, and Snapchat has exploded. Adults and youth alike utilize social networks to connect with friends and relatives and communicate with people who share common interests. Typically, individuals will create an account and profile. Profiles contain information and may be made public or private. Public profiles can be viewed by anyone who is a member of the same network and includes information, posts, pictures and anything else included as part of the individual's profile. Private profiles are shared with only those individuals who are "friends." A friend is described as someone who has requested to be your friend and has been accepted, thereby being allowed access to your information. Social network "friends" are not always real friends but rather people you agree to allow access to you via the social network. It

Paducah sex offender arrested for violating probation, using Facebook.

is not unusual for children, and even adults, to have many social networking "friends" they may have never met in person or have not seen in years. Young children in particular may not understand the difference between a real friend and a social networking friend.

Tips for All Users:

- Research and use privacy settings. They control who may or may not see posted information. Check these settings often.
- Use the same manners and language on social networking sites you use in a face-to-face social setting.
- Only accept "friends" you personally know. Would you allow a stranger in your home or in your desk to access your personal information? Social network friends are strangers and while you may think they are well intentioned, you really have no idea of their motives.
- Only post information or photos you are comfortable sharing with friends, teachers, parents, current and future employers, law enforcement or any other individual. What is put on the internet stays on the internet.
- Protect your passwords and usernames. Do not share this information with anyone.

• Parents should monitor social networking sites and further supervise the activity by becoming "friends" with their children on these sites, but be aware this will not ensure you see all activity.





Signs your children may be at risk...

They spend large amounts of time using technology.

Most children falling victim to online sex offenders spend large amounts of time online. Predators take notice of when children are home alone and will often communicate during those times to avoid adult interference.

They receive mail or packages from someone you don't know.

It is common for offenders to send letters, photographs, and gifts to their potential victims. They have even sent plane tickets for the child to travel to meet them.

They use an online account belonging to someone else.

Sex offenders will sometimes provide potential victims with an account used solely for communication with the offender. They will also teach children how to delete history, messages and to deactivate parental controls.

You find pornography on their computer or devices.

Sex offenders often supply their potential victims with pornography or suggestive material as a means of opening sexual discussions. Remember, this is part of the "grooming" process and often occurs after the predator has spent time forming a "relationship" with the child.

They turn the computer monitor off when someone enters the room or use other devices in private.

This may be an attempt to hide something. If this occurs, check the history and share your concerns with your child.

They become withdrawn from the family.

Predators work hard to drive a wedge between a child and his/her family. They will focus on even minor problems a child is having at home.

They make and receive phone calls to and from people you don't know.

Oftentimes sex offenders want to talk to the child on the phone, as well as online. They sometimes engage in "phone sex" and may seek to set up an actual meeting for real sex. They have been known to set up toll-free 800 numbers, so their potential victims can call them without their parents finding out. They may have a child call collect or send a child a cell phone that can be used for private communication.

What to do if you suspect your child is at risk online...

Talk about it. Let your children know you are concerned and it is your job to keep them safe. Give them the opportunity to discuss any potential or actual victimization without fear of getting in trouble.

Review what is on your child's computer and other devices. If you don't know how to do this, ask for help from a friend, coworker or relative. Explore all internet history and activity as well as email and social networking sites.

Closely monitor your child's internet usage on the computer, cell phone or other handheld device. Set very clear boundaries that allow for close monitoring and supervision. Stick to the boundaries you have set. Continue to have open communication with your youth. Continue to remind him online supervision is not punishment, but rather your job and duty as a parent wanting to keep him safe.







Internet Fraud: What are the dangers?

Internet fraud is the use of internet services to take advantage of someone else; most commonly identity theft. Identity theft occurs when someone assumes your identify to perform a fraud or other criminal act. Criminals can get the information they need from a variety of sources. Children can be victims and they should understand the risks.

> Tips to minimize risk of identity theft as an adult:

- Never throw away ATM receipts, credit statements, credit cards or bank statements. Always be sure to shred them. Never give your credit card number over the phone unless you • make the call.
- Review your bank account monthly and notify your bank of any problems.
- Keep a list of telephone numbers to call and report the loss or
- theft of your wallet, credit cards, etc. Review a copy of your credit report at least once a year.

Tips to minimize risk of identity theft for your children:

Teach your children to always keep their personal information safe, i.e. child's date of birth, social security

Never share personal information on the internet such as number, etc. their address or a picture of their driver's license. As they get older, teach them to always log out of any site that requires a user ID and password when they are finished.

Talk with them about the importance of safely disposing of any documents that may have personal information included.



Reports of Bullying in Kentucky's Public Schools Triple in 3 Years

Cyber-Bullying

Unfortunately, the internet, cell phones, text messaging and social media offer new ways for children to be hurt by their peers. Cyber-bullying can permeate every aspect of a child's life beyond the more traditional places such as the school bus or playground. Oftentimes, youth do not consider this type of interaction to be harmful, but rather a form of joking around. Sadly, they may not realize their actions can have irreversible, life-changing and even fatal consequences. Cyber-bullies have a variety of options and tools when it comes to victimizing someone. They include:

- Sending offensive, threatening or hurtful messages
- Stealing passwords to access social network profiles and other accounts to obtain information meant to be private
- Creating websites meant to tease, taunt and humiliate the victim
- Sending or forwarding embarrassing pictures through e-mail, social network sites and cell phones
- Internet polling (asking people to answer a mean-spirited question regarding someone) to tease and humiliate them
- Sending pornographic material via email or social networks
- Using impersonation to make it look as though the victim was sending messages or posting information or to trick someone into revealing personal information

Using responsible and safe online behavior can prevent some types of cyber-bullying. Keeping personal information private and protecting usernames and passwords can stop someone from using it to hurt or embarrass. Despite responsible behavior and parental monitoring, cyber-bullying can still occur. It can often be an extension of taunting and teasing going on at school.

It is important to teach youth how to respond to cyber-bullying and where to seek help. They need to know it is not their fault, and parents need to understand that revoking a child's online access as a result of cyber-bullying may make him hesitant to communicate about what is going on. An effective approach to deter the bullying is to report incidents to teachers, school resource officers and school counselors.



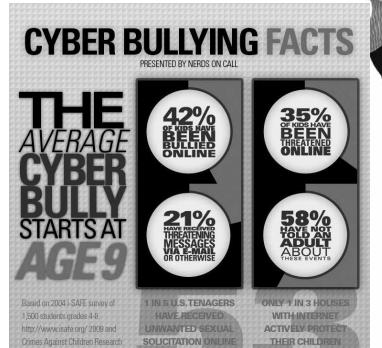


Cyber Bullying: on the flip side...

It would be a safe bet most parents want to protect their children from being bullied. How many parents, however, take the time to consider their child may be the aggressor? While it is of critical importance to teach youth how to protect themselves online, it is equally as important to teach youth cyber-bullying is a serious offense that goes beyond joking or teasing and it will not be tolerated.

Prevention tips for parents and caregivers

- Model appropriate online behavior
- Establish an atmosphere of mutual caring and trust within the home
- Help your child to understand the pain the victim feels. Share real examples so they understand how even joking can be hurtful
- Describe acceptable behaviors vs. aggressive behaviors
- Impose and enforce consequences for aggressive online and other behavior
- Have the bully take responsibility for his/her actions
- Seek help from a teacher, Family Resource Youth Services Center, doctor or professional counselor should the aggressive behavior continue



Parents and educators need to be reminded cyber-bullying can be emotionally destructive, cause anxiety or depression or cause the victim to seek revenge in a manner which creates more problems. Youth need to be supported, and in some cases, professional counseling should be sought to help identify and implement coping strategies.

When facing such difficult situations, the child and family should avoid isolation and seek support and assistance. Contact your child's Family Resource Youth Services Center or call 1-800-CHILDREN to access information regarding counseling or mental health services in your local community.



True or False?

Children using technology for any activity must understand the following statements are NOT TRUE. Discuss these statements with your child and use them as a conversation guide.

Information on the internet can always be trusted as factual—it wouldn't be online if it were not true.

Anything I send in my private email, Instant Message (IM) or chat cannot be seen by anybody other than to whom I sent it.

It is not against the law to take a sexual picture of myself and send it to my boyfriend. Or, it is ok for me to show my friends nude pictures of my girlfriend she took of herself and sent to me.

If someone I meet online asks me to keep a secret from my parents, I should.

If I meet someone online and he asks to be added to my "friend list" I should accept, because we are friends.



A website must have my permission to put any personal information about me, like my phone number, address or birth date, online.



If I want to know something about a stranger who sends me an IM, I can check their profile and trust that information.



Installing blocking software and a virus checker on my computer will keep me safe.

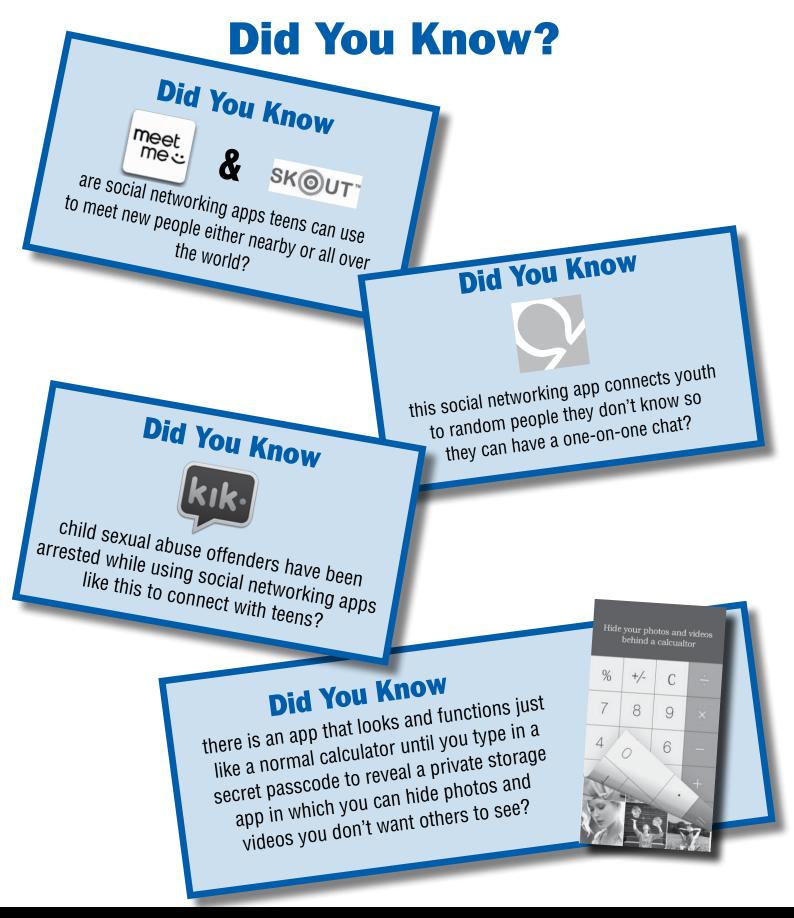


I can always trust emails and attachments I get from friends.

I'm visiting a site of an organization I've heard of before—it is okay to give my name and phone number to enter a contest.









Sample Safety Pledge

Safety pledges can help provide clear guidelines for safer internet use. NetSmartz recommends using the Internet Safety Pledge to promote safety discussions and create safer boundaries. Sample pledges for various ages can be found at

www.netzsmartz.org/Resources/Pledges#Primary.

Adult's Pledge

- I will set reasonable rules and guidelines. We will discuss these rules and I will monitor compliance.
- I will not overreact if a child tells me something about a problem he or she is having online.
- We will work together to solve problems and prevent them from happening again.
- I will be a good role model online.

Youth Pledge (Middle/High School):

1. I WILL THINK BEFORE I POST.

I agree not to post information and images that could put me at risk, embarrass me, or damage my future, such as

- Cell and home phone numbers
- Home address
- Sexual messages
- · Inappropriate pictures and videos

2. I WILL RESPECT OTHER PEOPLE ONLINE.

I will not

- Post anything rude, offensive or threatening
- Send or forward images and information that might embarrass, hurt, or harass someone
- Take anyone's personal information and use it to damage his or her reputation

3. I WILL BE CAREFUL WHEN MEETING ONLINE FRIENDS IN PERSON.

I agree to

- Ask my parent or guardian's permission before going
- Have a parent or guardian accompany me
- Meet in a public place

4. I WILL PROTECT MYSELF ONLINE.

If someone makes me feel uncomfortable or if someone is rude or offensive, I will

- Not respond
- Save the evidence
- Tell my parent, guardian, or another trusted adult
- Report to the website, cell phone company, CyberTipline.com, or the police

Signature:

Date:

Signature:

Date:





Additional Resources

www.pcaky.org

Prevent Child Abuse Kentucky offers additional resources and templates, as well as statistics and information on other forms of child abuse and neglect; prevention trainings on a variety of topics are also available.

www.missingkids.com

The National Center for Missing & Exploited Children, (NCMEC), serves as the nation's resource on the issues of missing and sexually exploited children. The organization provides information and resources to law enforcement and other professionals, parents and children including child victims.

www.cybertipline.com

Report child pornography or suspected child sexual exploitation.

www.ncpc.org

The National Crime Prevention Council has downloads for parents, including a cell phone use contract and parent tip sheet.

www.dhs.gov/stopthinkconnect

The Department for Homeland Security offers messages and tools to promote responsible internet use and awareness of fraud, identity theft, cyber predators and cyber ethics.

www.netsmartz.org

A program of the National Center for Missing and Exploited Children that has resources for parents/guardians, educators, law enforcement, teens and kids about safe internet use.

www.netsmartz411.org

Offers an "ask the expert" section that can help parents navigate software, websites, commonly used acronyms, etc.

www.facebook.com/help

The Help Center allows users to find information regarding the site's products and policies, including answers to frequently asked questions and step by step guides for configuring security settings.

www.kentuckystatepolice.org/kicactf/icactf_index.html

Kentucky State Police Internet Crimes Against Children Task Force

www.ag.ky.gov/criminal/dci/cybercrimes/Pages/default.aspx

Kentucky Attorney General Cyber Crimes Unit

www.justice.gov/usao-edky/project-safe-childhood

United States Attorney's Office Project Safe Childhood

Search engines such as **www.google.com** often help translate messaging or chat shorthand.

Websites such as **www.chatslang.com** or **www.netlingo.com** provide an extensive list of text, instant messaging and chat shorthand.



Prevent Child Abuse Kentucky thanks the Child Victim's Trust Fund for supporting the revision of this important resource. We also thank staff from the Attorney General's Office, Kentucky State Police Electronic Crimes Branch and the United States Attorney's Office, Eastern District of Kentucky for their contributions to this project.





801 Corporate Drive, Suite 120 Lexington, Kentucky 40503

> 859-225-8879 Fax 859-225-8969

1-800-CHILDREN

pcaky@pcaky.org www.pcaky.org



© 2016 Prevent Child Abuse Kentucky. All rights reserved. Please contact us at pcaky@pcaky.org to request permission to reproduce this information. This project is funded in part or in whole with state or federal funds through a contract (#PON2 736 1600001309) with the KY Cabinet for Health and Family Services