



internet safety TOOLKIT



Prevent Child Abuse
Kentucky

TABLE OF CONTENTS

2	Youth and technology
3	What can we do?
5	Help with the uncomfortable conversations
6	Social networking
7	Signs your child may be at risk
8	What to do if you suspect your child is at risk
9	Phone safety
11	Sexting
13	Cyber-bullying
15	True or false
16	Additional resources



Internet Safety

A toolkit to help children stay safe

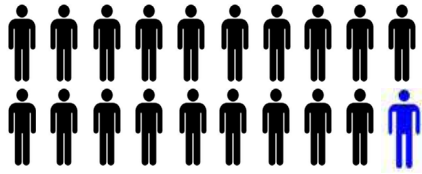
The Internet offers a world of possibilities to children and has become an important part of their every day life. It provides information about almost anything; it is used in education, used to communicate and is great entertainment. Our children are learning how to utilize technology at a very young age. Often times, their technology skills are greater than those of adults.

While technology is good, it also has a negative side. It provides frightening opportunities for children to be exposed to the risk of unwanted or unsafe material, to predators who are unyielding in their efforts to manipulate them and other potential harm.

There is good news! Children and adults can safely use technology, avoid risks, and cope with unsafe situations, if they arm themselves with information and skills to do so.

This Tool Kit, created in collaboration with experts from across the state of Kentucky, will help provide information needed to keep children safe.

Youth and Technology



95% OF ALL TEENS ARE ONLINE



80% OF THOSE TEENS USE SOCIAL MEDIA

TEENS SPEND AN AVERAGE OF 5 HOURS PER DAY ONLINE

WHERE KIDS SAY
THEY SPEND THEIR
TIME ONLINE



82%
Schoolwork



76%
Social Media



73%
Email



63%
Games



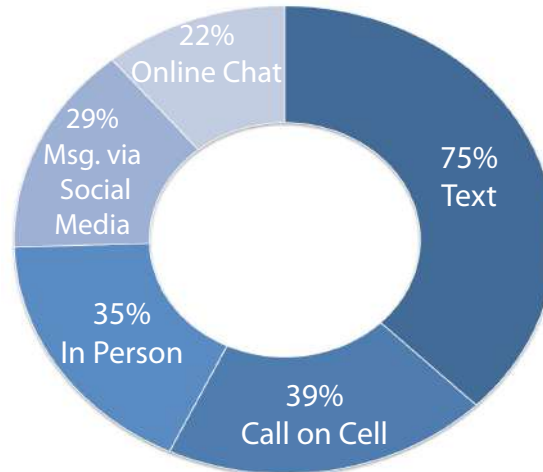
25%
Chat



23%
Music/ Movies

70% OF TEENS ADMIT TO HIDING THEIR ONLINE
BEHAVIOR FROM THEIR PARENTS

AT ANY GIVEN
TIME, IT IS
ESTIMATED A
HALF MILLION
PREDATORS
ARE ONLINE
PROWLING FOR
CHILDREN



HOW TEENS SAY
THEY PREFER TO
COMMUNICATE

FACEBOOK IS THE 2ND MOST TRAFFICED WEBSITE IN THE
WORLD BEHIND GOOGLE



85% of ALL users
online have
Facebook

1 IN 5 TEENS HAVE
ENGAGED IN SEXTING



What can we 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 are in control
- Things you read online may be untrue

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

Be aware the internet is accessible on home computer, phones, gaming devices, iPod touch, iPad, TV, etc. Do not allow internet usage to be a private matter. However, since the internet can be used with no supervision, parents must know their children's usernames and passwords for all online accounts.

Model appropriate behavior. The truth is, 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 of and/or by youth. Did you know, if a child takes a photo of themselves naked, they could be guilty of producing pornography? Did you know if you find a photo of child that is naked and 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 child knows what to do in the event something happens as a result of online activity. Adults and children will respond more appropriately if there is a plan.

Communicate, communicate, communicate! Do not just rely on parental controls. While they are important tools, your children will have Internet access where there are no parental controls in place.

- Talk to them about positive aspects of Internet use as well as the dangers.
- Have discussions about how child predators may go online to exploit or victimize youth. Discuss how actions can lead to victimization and lead to irreversible consequences.
- Kids must realize things they see online may be untrue and they may be communicating with someone who is not who they say they are.

"Many times, online predators do not lie about their age or who they are. They meet the needs of their potential victim by listening to them, understanding them, offering them advice. They become a real friend to the child they have targeted."

—DETECTIVE DAVID
FLANNERY
Internet Crimes
Against Children,
Lexington Division of
Police

"Teaching kids online safety should be right up there with teaching them about the birds and the bees and drugs."

—KYLE EDELEN
U.S. Attorney Office
Eastern District of
Kentucky

Communicate regarding these issues on a regular basis. Don't wait for something to happen to have these discussions.

Review age appropriate online safety material with your children such as resources found at www.netsmartz411.org.

Set guidelines with first use. By doing so, responsible behaviors and habits are established from the very start.

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

Learn chat and messaging shorthand. 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 activity.

Understand chatting, instant messaging, and texting allow for real time dialogue between two or more people. Parents must know how it works and what measures can be taken to monitor the activity.

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 prowling. 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 upload (post) pictures online without permission and explain why.
- Never request or agree to a face-to-face meeting with someone met online even if a relationship has been established and explain why.
- 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 and tell someone when this is happening.
- Set limits and guidelines on technology usage early. 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 they are illegal and can be utilized to distribute child pornography.

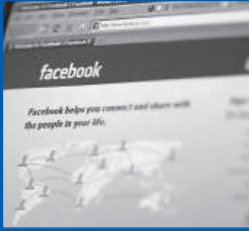
Help with the uncomfortable conversations

- Start conversations with initial use of technology & 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 not to let 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.
- Use current events to begin a conversation.
"Did you see the news story about (insert title of recent adult scandal)? Think about how the adults spouse/ parents/ children must feel. Talk about what the adult should have done differently.
- 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.
- 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).

"It is important to set limits and boundaries from the very beginning to prevent a child from feeling punished for having restrictions placed on their Internet use after an unsafe situation occurs."

—KELLIE KOZEE
WARREN
Prevent Child Abuse
Kentucky

Social Networking



"Many, if not most, of the crimes I have investigated began with a social networking site."

—DETECTIVE DAVID
FLANNERY

Internet Crimes
Against Children,
Lexington Division
of Police

The popularity of social networking sites 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. This includes information, posts, pictures and anything else that may be 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.

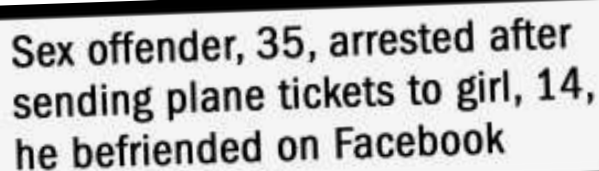
Tips for All Users:

- Research and use privacy settings. They control who may or may not see posted information. Check these settings often.
- Only accept "friends" you personally know. Would you allow a stranger in your home, in your desk, access to 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.
- Be cautious of what you post. Only post information or photos you would be 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.
- Use the same manners and language on social networking sites you use in a face-to-face social setting.
- Protect your passwords and usernames. Do not share this information with anyone except your parent or caregiver.
- 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 parents see all activity.



Signs your child 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.



Sex offender, 35, arrested after sending plane tickets to girl, 14, he befriended on Facebook

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.

Computer-sex offenders will sometimes provide potential victims with a computer account that is used solely for communication with them. They will also teach children how to delete history, messages and to deactivate parental controls.

You find pornography on their computer.

Sex offenders often supply their potential victims with pornography not only as a means of opening sexual discussions but also for seduction. This material may be stored on a hard drive or on memory sticks (digital data storage technology). Remember, this is part of the "grooming" process and often occurs after the predator has spent a great deal

of time forming a "relationship" with the child.

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

Doing this or quickly changing the screen on the monitor may be an attempt to hide what is being looked at on the computer. If this occurs, check the history and share your concerns with your child.

They become withdrawn from the family.

Predators will 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 computer-sex offenders will 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.

"In most cases I have prosecuted, children go to meet the predator willingly. They see this person as someone with whom they have a bond (a boyfriend or best friend) and not a stranger."

**—ERIN MAY ROTH U.S.
Attorney's Office
Eastern District of
Kentucky**

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

Knowing a child's username and password could save their life in a situation where they have gone to have a face-to-face meeting.

Talk about it.

Let your child know you are concerned and it is your job to keep him safe. Give him 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, co-

worker 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 your child safe.

ALWAYS REPORT SUSPICIOUS ACTIVITY

1. Communicate your concerns to all adults living in the home so they may assist in monitoring activity.
2. Communicate your concerns to your child's teacher, principal and/or school counselor so that monitoring will continue at school.
3. Contact your local police department or the Kentucky State Police regarding your concerns.
4. Contact The Center for Missing & Exploited Children at 800-THE-LOST (800-843-5678) for help and information or go to www.cybertipline.com to report concerns. Tips can be made anonymously.

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 a home. Now, children can 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. Make sure your child knows how to use the phone in emergency situations and make sure you are equally as skilled at using the phone and reviewing phone usage.

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. Talk to your child about with whom they are communicating. Look for changes in patterns.

Communicate with your child how talking on the phone can cause her to be distracted and less aware of her surroundings. Remind them people can hear what they are saying when speaking in public, including child predators who may be listening to their conversation.

Warn your child about the dangers of texting while driving. Set a good example. It is against the law.

Limit Internet access on cell phones. As

already mentioned, online activity needs to be monitored. Online activity cannot be closely monitored if it can be accessed via cell phone or other handheld device.

Consider deactivating the camera feature on your child's phone. The absence of a camera will not limit communication, however, it will prevent inappropriate pictures being taken and sent via text.

Learn the lingo. There is a rapidly growing shorthand used when texting and instant messaging. Learn and keep up with this language.



Pay attention to child's behavior as it relates to texting. For example, is the child being more secretive regarding texting?

Set limits and be consistent. Make sure your child understands continued cell phone use is contingent upon following the rules. Limits should include:

- Never talk or text with people who you do not personally know. Remember, children may not consider their online friends as "strangers," however, you must be clear that phone communication is not allowed with these individuals despite any online relationship.
- Never discuss personal information in public. A child predator can gain a wealth of information—such as child's school and address—from eavesdropping.
- Place a curfew on cell phone usage. Having possession of the phone at night will give parents the opportunity to review phone activity; and also prevent late night calls and texts. Start this rule from the beginning.
- Have an honest discussion about concerns and risks and have a plan for unusual calls or texts. It is important your child knows what to do in the event he/she receives any type of harassing, threatening, sexually explicit or bullying calls or text messages. They need to understand by telling you, the two of you can work together to resolve the situation.
- Maintain zero tolerance for sexting and be honest regarding potential legal troubles.

SAMPLE SAFETY PLEDGE

PARENTS' 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.
- I will be a good role model online.

YOUTH PLEDGE

- I will be respectful to myself and others.
- I will not bully and won't tolerate bullying by others.
- I will not post or send pictures or other content that could embarrass me/ others, get me in trouble or jeopardize my security.
- I will tell an adult if I (or a friend) find myself in a difficult situation online.

FOR A COMPLETE COPY
OF THE FAMILY CONTRACT
TEMPLATE, LOG ON TO:

WWW.PCAKY.ORG

Sexting

Sexting is sending sexually explicit messages or photographs between mobile phones or other handheld devices; it is a popular 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 will have consequences well beyond embarrassment and the potential for exploitation.](#)

Youth need to understand the seriousness of sexting. Sending or receiving sexually explicit photos via mobile phones or other handheld devices (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. for 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 (this includes any sexually explicit photos of children under 18—even if it is of yourself) and inability to gain future employment.

Children may not fully realize that their best friend in middle school may be their worst enemy in high school. They need to be taught the consequences of trusting people not to share their pictures or texts.

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.
- Communicate openly about potential or actual victimization (including bullying, harassment, and threats).
- Report any suspected illegal interaction with adults to your local law enforcement agency or Kentucky State Police.
- Take the phone or limit access.

Cyber-Bullying

There have been far too many news reports about cyber-bullying and irreversible, life changing and even fatal consequences. Bullying is not a new issue. Unfortunately, the Internet, cell phones, text messaging and social media offer new ways for children to be hurt by their peers. Oftentimes, youth do not consider this type of interaction to be harmful, but rather a form of joking around. Sadly, they may not realize the negative impact of their actions until it is too late.

Cyber-bullying is a term generally used to describe using technology to send, text or post images intended to harass, threaten, embarrass or otherwise hurt another person. 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 access information meant to be private.
- Using blogs to write and to spread rumors or make fun of them.
- 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 that is 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.



Cyber-bullying is widespread with one-third of teens having experienced it, engaged in it or know of friends who have done either.

An effective approach to deter the bullying is to teach kids how to block messages and/or delete messages without reading them.

They can also report bullying incidents to Internet Service Providers (ISPs), website monitors and social networking sites.

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 that creates more problems for the victim. 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.

O.C.L.C.

One Click Lifetime
Consequences

Only you can make
a choice to prevent
one click from
being a lifetime
consequence.



Cyber-Bullying: on the flip side...

“Communication is essential as we work to keep kids safe.”

—JESSICA FLETCHER
Training Resource
Center Associate
Director, University of
Kentucky

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 & 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 behavior vs. aggressive behaviors.
- Impose and enforce consequences for aggressive online 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.

True or False?

If your child uses modern technology for any activity, he must understand the falsehood of the following statements. Consider reviewing these statements with your child and using it as a guide for conversation regarding safe use of technology and the potential risk for danger.

1. Information on the Internet can always be trusted as factual—it wouldn't be online if it were not true.
2. Anything I send in my private email, IM or chat cannot be seen by anybody other than to whom I sent it.
3. There are no legal ramifications of taking a provocative picture of myself and sending it to my boyfriend. Or, it is ok for me to show my friends nude pictures of my boyfriend that he took of himself and sent me.
4. If someone I meet online asks me to keep a secret from my parents, I should.
5. If I meet someone online and he ask to be added to my "friend list" I should, because we are friends.
6. A website must have my permission to put any personal information about me online, like my phone number, address or birth date.
7. If I want to know something about a stranger who sends me an Instant Message, I can check their profile and trust that information.
8. Installing blocking software and a virus checker on my computer will keep me safe.
9. I can always trust emails and attachments I get from friends.
10. 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.

"Remember, children have access to technology at a very young age, and the risks they face are different at different ages. It is critical parents and caregivers have ongoing conversation with youth regarding these risks."

—JOEL GRIFFITH
Prevent Child Abuse
Kentucky



Additional Resources

www.pcaky.org Prevent Child Abuse Kentucky offers additional resources and templates as well as statistics and information on child abuse and neglect prevention.

www.missingkids.com The National Center for Missing & Exploited Children, (NCMEC), serve 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.

<http://www.facebook.com/help> The Help Center allows user 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.

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.

Sample Text, Instant Messaging and Chat Shorthand	
8	Oral sex
143	I love you
182	I hate you
1174	Nude club
420	Marijuana
AEAP	As early as possible
ALAP	As late as possible
A/S/L	Age/sex/location
CD9	Code 9: parents are around
F2F	Face to face
GNOC	Get naked on camera
GYPO	Get your pants off
KPC	Keep parents clueless
LMIRL	Let's meet in real life
PRON	Porn
PIR	Parent in room
S2R	Send to receive (picture)
zerg	To gang up on someone



Prevent Child Abuse
Kentucky

Prevent Child Abuse Kentucky thanks the UPS Foundation for the funding provided to continue the Internet Safety Tool Kit Training Project.

A special thank you also goes to the members of the Community Partner Workgroup for their hard work, insights and valuable contribution to the initial project.

Community Partner Workgroup Members

James Johnson
Office of the Attorney General

Allison Dickinson
Glasgow Independent Schools

Audrey Brock
Department for Community
Based Services

Wm. Allen Love
United States Attorney's Office
Eastern District of Kentucky

Lee Ann Gabbard
Family Resource and Youth
Services Centers

Crystal Barger
Eastern Kentucky University

David Flannery
Internet Crimes Against
Children Detective, Lexington
Division of Police

Frank Kubala
Department of Criminal
Justice Training Center

Jessica Fletcher
University of Kentucky
Training Resource Center

Missy Segress
University of Kentucky
Training Resource Center

Erin May Roth
United States Attorney's Office
Eastern District of Kentucky

Kyle Edelen
United States Attorney's Office
Eastern District of Kentucky



Prevent Child Abuse
Kentucky

801 Corporate Drive, Suite 120
Lexington, KY 40503

859-225-8879
Fax 859-225-8969

1-800-CHILDREN

pcaky@pcaky.org
www.pcaky.org

facebook.

/PCAKY

twitter

@pcaky