



*"Creating Safer Schools.....Building by Building"
"Creando Escuelas Seguras.....Escuela Por Escuela"*

New York State Center for School Safety
175 Route 32 North
New Paltz, NY 12561
Phone: 845-255-8989
Fax: 845-255-3836
E-mail: scss@ulsterboces.org
<http://nyscenterforschoolsafety.org>

March 2006

FACT SHEET

Cyberbullying

by Sherry Runk

Informational technologies or cybertools can be used in many positive ways, but they are also being used to harm or hurt others. This hurtful behavior is often not happening in schools but occurs in what used to be the safety of one's own home. Youth who are the victims of cyberbullying are asking: "Am I safe anywhere?" Since cybertools, especially social networking sites, are quickly becoming the social venue used by youth, to help develop and maintain relationships with friends and family, it is important to understand cyberbullying, the difference between face-to-face bullying vs. cyberbullying, and to know what can be done to minimize how technology can be used to cause widespread hurt to others in a matter of seconds. Teens avoid challenging or angering a cyberbully for fear of online retaliation that can cause emotional harm and embarrassment, destroy reputations or damage future work or educational plans. Cyberbullying is rapidly increasing and we must work together to prevent further pain inflicted by it.

What is cyberbullying?

Willfully causing hurt or harm verbally, emotionally, or psychologically to another person by using cybertools and other informational technologies by sending threatening or violent messages that:

- Intimidate
- Threaten
- Impersonate
- "Cyber" stalk
- Bully
- Ridicule
- Humiliate
- Trick
- Harass
- Tease
- Generate Rumors

What are cybertools?

- E-mails
- Blogs & Vblogs
- Text Messages
- Discussion Groups
- Online Video Games
- Web Sites
- Camera Phones
- Listserv
- Cell Phones
- Peer-to-Peer Networking
- Instant Messages (IM)
- Digital Images
- File-Sharing
- Message Boards
- Chat rooms

How is cyberbullying different from other forms of bullying?

- Creates an illusion of anonymity: Cyberbullies cannot see their victim/s or the resulting harm or pain caused towards others; and the recipient does not know whom to trust.
- Imposed consequences are minimal or non-existent for hurt or harm inflicted on others when cybertools are misused

because often the person who bullies is often unknown.

- Use of high-speed technology can quickly disseminate harmful messages to a large number of people.
- Ability to identify a cyberbully is difficult.
- Notifying service providers and the follow up to a cyberbullying incident can take lots of time.
- Offers a venue for the person who encounters face-to-face bullying to retaliate anonymously online to the person/s who did the bullying.
- Has the ability to quickly connect and expand a circle of friends and groups on-line who are irresponsible and or have antisocial behavior that can cause widespread harm to others.
- Creates the opportunity to adopt an on-line identity.
- Cyberbullying can be done online by a "less powerful" person against a "more powerful" person; the imbalance of power differs from other forms of bullying.
- Does not contain the physical aspect of other types of bullying.
- Can be more emotionally damaging.
- Has exposure to a greater number of sexual predators.
- Can occur 24/7.

What is the impact on the victim?

- Low self-esteem
- Anger
- Fear or Intimidation
- Depression
- Suicide
- School Violence
- Anxiety
- Smoking/Drinking
- Lower school attendance and
- achievement,
- School failure or drop in grades
- Increased social isolation

The impact of cyberbullying may be stronger than face-to-face bullying. The home is no longer a safe haven, messages sent can be meaner, more harmful, and can reach a large number of people in real time; thus having an intense impact on the victim. Some online social norms can support and/or encourage cyberbullying and risky or irresponsible behavior.

What can be done?

Parents/Guardians:

- Keep the computer in a room in your house that is not isolated so computer activities can easily be monitored.
- Talk with your child about cyberbullying and correct cybertool netiquette, focusing on values of being kind and respectful.

- Discuss the concerns of public disclosure of intimate personal information.
- Model appropriate use of cyber tools.
- Teach your child that computer identities can be traced.
- Consider using an Internet Service Provider that offers restricted child access or use filtering or blocking software.
- Have your child demonstrate how to navigate websites, use chat rooms, or other cyber tool functionality, especially if you have minimal computer knowledge.
- Know the websites your child visits and encourage them to discuss their online experiences with you.
- Watch for behavioral signs from your child who doesn't want you to see what is on the monitor, like minimizing the screen when you walk into the room.
- Impose appropriate consequences when your child misuses cyber tools, e.g., loss of use of computer or cell phone.
- Know that teens feel that parents do not understand or know how to respond to cyberbullying and fear their internet access will be unfairly limited if incidents are reported.
- Learn about teenage Internet lingo by going to www.netlingo.com (e.g., Free to Talk-F2T; Best Friends Forever-BFFs; Parents Are Watching-PRW; or Too Late-2L8.)

Educators:

- Develop, distribute, and update annually school cyber tool, and bullying rules, policies, and procedures.
- Include cyberbullying in workshops for both students and staff.
- Model respectful, empathetic and positive behaviors, and attitudes.
- Teach effective problem-solving skills.
- Educate students that cyber tool users are not anonymous and that their online activities and files have limited privacy: computer information can be downloaded, Internet Protocol (IP) addresses are generated and used for tracking, and communications can be traced.
- Educate students that there are limits to their free speech rights when posting or disseminating online materials.
- Encourage students to report known incidents of cyberbullying and provide confidential means to report cyberbullying.
- Inform students that cyber tool misuse may be considered criminal acts and punishable by law.
- Let bystanders know that they can help stop cyberbullying behavior and that ignoring it can encourage cyberbullying behavior; support targets of cyberbullying.
- Create Situation Review Team/s to review and investigate reports of cyberbullying.
- Use filtering and tracking software.
- Know that pornography can easily be accessed by children yet is to be legally restricted to adults and that pedophiles have direct one-to-one access to our youth.

Youth:

- Do not share personal information or your password.
- Do not post your picture or use screen names that can reveal personal information on the internet.
- Watch for the following signs when receiving messages from others you don't know well and if they happen, tell an adult; print the message and do not delete it:

- ⇒ asks for a lot of information from you, yet offers little in return,
- ⇒ sends you lots of messages and lots of compliments,
- ⇒ asks for photos and personal or private information, and
- ⇒ requests to meet you in person (never go without parent/guardian's permission).

- Do not open e-mails from strangers and do not open unknown attachments.
- Look for a privacy policy on visited websites when information is requested from you.
- Refrain from sending messages when angry or responding to bullying messages.
- Ignore a bully's email, text messages and other forms of cyberbullying messages.
- Report to an adult if in receipt of an inappropriate, anonymous message, a threat, or other upsetting materials to see if the message can be traced through the Internet Service Provider.
- Block any numbers or e-mail addresses that send offensive messages.
- Know that cyberbullying causes pain and harm to others who are "unseen".
- Use discernment regarding the information received via cyber tools because people misrepresent who they are and can send false messages or information.
- Use social networking sites responsibly.
 - Set your profile to private (this controls access) but know others could still have access so use caution with information shared, and personal information posted, online.
 - Post appropriate pictures and discuss appropriate topics because this information can end up on the Internet or other kids' profiles.
 - Know that predators can find you by the information you post; AVOID posting any personal information like your address, school, siblings, etc.
 - Know you may be held accountable for inappropriate information posted; schools are developing policies to allow disciplining for online behavior, even if written at home, and some inappropriate information is against the law. Note that messages via cyber tools that might be perceived as a serious threat may result in suspension, expulsion, or even arrest.
- Call 1-800-843-5678, National Center for Missing and Exploited Children if exposed to child pornography and inform an adult.
- Report harassment to the Federal Bureau of Investigation (FBI) 602-279-5511.

Observer or Bystander:

- Support the victim in private or in front of the bully
- Tell the bully to stop the cyberbullying behavior
- Tell an adult about the cyberbullying incident

What are the guidelines for contacting law enforcement?

If threats are:

- Death threats
- Violent
- Sexually exploitive
- Discriminatory (race, religion, gender, sexual orientation, etc.)

- Engaging in extortion or coercion
- Obscene or harassing text messages
- Hate or bias-based
- An image of someone in a place where privacy is expected
- Material considered harmful to minors or child pornography

What are some of the cybertool definitions?

- **Cyberspace**-The online world of computer networks and especially the internet (www.m-w.com/)
- **Flame**-An online, short-lived fight using electronic messages with angry and vulgar language. (An Educator's Guide to Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, threats and distress by Nancy Willard) A longer message is called a "flame war".
- **Harassment**-A repeated, one-sided nasty, mean, and insulting message to an individual target usually through a cyberbully's personal communication channels including e-mail, instant messaging and text messages (Cyberbullying and Cyberthreats by Nancy E. Willard)
- **Disinhibition**-Possess little or no restraint on cyber messages sent to others; will do/say things in cyber space that one is unlikely to do or say in person.
- **Cyberstalking**- Cyberstalking can be defined as threatening behavior or unwanted advances directed at another using the Internet and other forms of online and computer communications. (National Center for Victims of Crime) Repeated, intense harassment and denigration that includes threats to create significant fear.
- **Cyberthreats**- Direct threats or material that raises concerns a young person may engage in an act of violence against others or self disseminated using the Internet or other information communication technologies. (Center for Safe and Responsible Use of the Internet; Nancy Willard, 2005)
- **File-Sharing**- (also known as "peer to peer" technology) allows you to search for and copy files directly from the computers of others. The most common use of this technology is to swap digital music files (MP3s), movies and TV shows. (Media Awareness Network)
- **Blogs**-A web page that serves as a publicly accessible personal journal for an individual. (www.webopedia.com)
- **Denigration**-Information that is harmful, untrue, or cruel that is posted online or sent to others to usually interfere with friendships or damage the reputation of another. "Dissing" someone online. (Cyberbullying and Cyberthreats by Nancy E. Willard)
- **Impersonation**-The cyberbully gains access to another's password or uses other cybertools to pretend to be another person (the person who is cyberbullied) with the intent of hurting friendships or harming the target in some way. (Cyberbullying and Cyberthreats by Nancy E. Willard)
- **Outing**-Publicly posting, sending or forwarding online someone's secrets, embarrassing information, or images. (Cyberbullying and Cyberthreats by Nancy E. Willard)
- **Trickery**-Tricking someone into revealing secrets or embarrassing information, then sharing it online.

If a hateful or harmful message is typed and the send button is depressed, it is too late to stop the message from reaching the recipient.

Cyberbullying Statistics

- 4,000,000+ children are posting content to the Web everyday.

- One in three teens and one in six preteens have been victims of cyberbullying (Fight Crime: Invest in Kids, 2006).
- The most common complaint from teens was about private information being shared rather than direct threats. Girls were more likely than boys to be targets and teens who share their identities online are the most vulnerable. (PEW/Internet)
- 35% of kids have been threatened online and nearly one in five have had it happen more than once. (i-Safe Survey).
- One in five child Internet users have received unwanted sexual solicitations yet only one in four have told a parent (National Center for Missing & Exploited Children).
- 34% of youth said they had unwanted exposure to sexual materials (YISS-2)
- 93% of parents say they have established Internet safety rules; 37% of students report that they have not been given any rules from parents on Internet safety.
- Webroot Software, Inc., a leading provider of security software for the consumer, announced research that shows a disconnect between parents and their children regarding Internet usage. While more than 70 percent of the children surveyed (ages 11 to 17) said their parents ask them about their online activities, the Webroot State of Internet Security Report unveiled a number of significant differences between child Internet activities compared to parent perception including:
 - Forty-five percent of children surveyed say they spend an average of three or more hours on the Internet daily while, according to the National Center for Education Statistics, 61 percent of all 13 year-olds spend one hour or less on homework; 76 percent of parents believe their children spend an average of two hours or less on the Internet;
 - Nearly 40 percent of children ages 11 to 17 reported they received a sexually explicit email or pop-up advertisement within the past year.
- 58% of kids admit someone has said mean or hurtful things to them online and more than four out of ten say it has happened more than once. (i-Safe Survey)
- 53% of kids admit having said something mean or hurtful things to another online. (i-Safe Survey)
- 58% of kids have not told their parents or any adult (i-Safe Survey)
- 42% of kids have been bullied while online and one in four have had it happen more than once. (i-Safe)
- 57% of profiles included at least 1 photo on "Myspace" (EMCC)
- 9% of profiles on "Myspace" included full name. (EMCC)
- 95% of parents didn't recognize the lingo kids use to let people know that their parents are watching. (EMCC)
- Most cyberbullying occurs within 9-14 years of age (Dr. Parry Aftab)
- 75% had visited a website bashing (Dr. Parry Aftab)
- 94 percent of young people access the Internet from home, with students as early as Grade 4 beginning to rely on the Internet to explore social roles, stay connected with friends and develop their social networks. (Young Canadians in a Wired World (YCWV) research project.) www.media-awareness.ca/english/research/YCWV/phaseII/upload/YCWV_trends_recomm.pdf
- About one third (32%) of all teenagers who use the internet say they have been targets of a range of annoying and potentially menacing online activities – such as receiving threatening messages; having their private emails or text

messages forwarded without consent; having an embarrassing picture posted without permission; or having rumors about them spread online.

References and Resources

1. **An Educator's Guide to Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats and Distress** by Nancy Willard.
2. **Center for Democracy & Technology** - www.cdt.org/legislation/105th/privacy/coppa.html
Information about Children's Online Privacy Protection Act (COPPA)
3. **Center for Safe and Responsible Internet Use** - <http://csriu.org/>
4. **Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the U.S. Department of Justice** - www.cybercrime.gov/
5. **Crimes Against Children Research Center** - www.unh.edu/ccrc/ Youth Internet Safety Survey Publications: YISS-1 and YISS-2
6. **Cyberbullying** - www.cyberbully.org/
Mobilizing educators, parents, students, and others to combat online social cruelty
7. **Family Guide Book** - www.familyguidebook.com/ (2004 by Parry Aftab, Esq.)
Help to understand the difference between what is annoying and what's a serious danger online.
8. **Federal Trade Commission** –
 - a. **Kidz Privacy-How to Protect Kids' Privacy Online** - www.ftc.gov/kidzprivacy/
 - b. **How To Protect Kids' Safety Online: A Guide for Teachers.**
9. **Fight Crime: Invest in Kids** - www.fightcrime.org/
10. **i-Safe America, Inc.** - <http://isafe.org/>
i-SAFE America Inc. is the worldwide leader in the Internet safety education
11. **Mind OH** – www.mindohfoundation.org/about.htm
The MindOH! Foundation seeks ways to increase the reach and impact of character education to motivate youth to practice moral and ethical.
12. **National Center for Missing & Exploited Children® (NCMEC)** - www.missingkids.com/
13. **National Center for Victims of Crime** - www.ncvc.org/ncvc/Main.aspx
14. **NetLingo**: NetLingo contains thousands of Internet communication definitions - www.netlingo.com/.
15. **Netsmartz** - <http://netsmartz.org/>
Lesson Plans for Teachers: The NetSmartz Workshop is an interactive, educational safety resource to teach kids and teens how to stay safer on the Internet.
16. **New York State Division of Criminal Justice Services** - www.criminaljustice.state.ny.us/missing/i_safety/cyberbullying.htm and http://criminaljustice.state.ny.us/missing/i_safety/i_intro.htm
17. **Office of Juvenile Justice and Delinquency Prevention and Internet Crimes Against Children (ICAC) Task Force Program** - www.icactraining.org/
18. **Parry Aftab, Esq.** - www.aftab.com/
Managing cybercrime, privacy and cyber-abuse risks; Contact parry@aftab.com or Telephone: 201-463-8663
Links to Parry Aftab's safety websites:
 - Wiresafety - www.wiresafety.org/
 - WiredKids - www.wiredkids.org/
 - Familyguidebook - www.familyguidebook.com/
 - The Cyber Law Enforcement Organizations

(www.cyberlawenforcement.org/)

19. **Project Safe Childhood** - <http://www.projectsafefchildhood.gov/>
20. **Safe and Responsible Social Networking, Tips for Adolescents**, Sameer Hinduja, Ph.D. and Justin W. Patchin, Ph.D.
21. **The Children's Internet Protection Act (CIPA)** www.legal-database.com/childrens-internet-protection-act.htm.
22. The Cyber Law Enforcement organization—www.cyberlawenforcement.org
23. FBI Parents' Guide to Internet Safety—www.fbi.gov/publications/pguide/pguidee.htm
24. New York State Cyber Security & Critical Infrastructure Coordination (CSCIC) - www.cscic.state.ny.us

Specific to New York State: The New York State Commission of Investigation Recommendations on Cyber Crimes Against Children, February 2007

Mary Grenz Jalloh, Executive Director of New York State Center for School Safety, had given testimony at a public hearing on the Discipline Codes and Filtering Software for the New York State Commission of Investigation on Cyber Crimes Against Children. The full report and her testimony are available on the Internet at www.sic.state.ny.us; the Commission's recommendations are as follows:

- Enact legislation that would define the word "depicts" to include both words and pictures.
- Institute graduated sentencing for child pornography offenses.
- Criminalize, as a class C felony, the act of enticing a child into an area or act by false promises or rewards, where the child's welfare would likely be endangered.
- Amend the Sex Offender Registration Act Scoring (SORA) for cyber predators.
- Allow the Business Records Hearsay Exception to apply to ISP records for purposes of grand Jury presentations.
- Institute mandatory, uniform, age-appropriate Internet safety curriculum throughout all public schools.
- Allocate more dedicated resources to assist in law enforcement efforts to combat Internet crimes against children.

Sherry Runk is a Senior Trainer
at the New York State Center for
School Safety.

