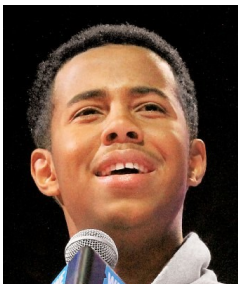
The Global StopCyberbullying Youth Summit—Ireland 2015

Our Special Guests and Friends

Senator Tony Mulcahy

Barbara Coloroso

Carol Todd



Mustafa Ahmed

May the road rise up to meet you. May the wind be always at your back.
May the sun shine warm upon your face: the rain fall soft upon your fields and until
we meet again, may God hold you in the palm of his hand.

Amazing People You Met at the Summit:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

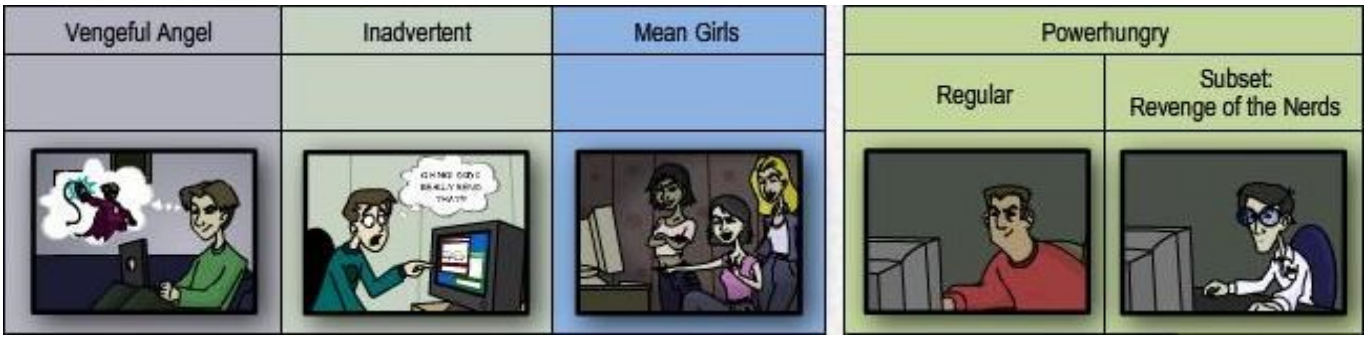
_____

_____

Time	Activity, Panel or Breakout Topic
8:45 – 9:15am	Welcome and Opening Ceremony
9:15 – 10:15am	Panel: Cyberbullying: How it Works, the Players, the Methods and the Motives
10:15 – 10:45am	Carol Todd – My Daughter Amanda
10:45 – 11:45	Breakout Sessions 1-6 Understanding the Risks and Identifying Cyberbullying Profiles
11:45 – 12:30pm	Panel - Special Risks: Vulnerable Groups, Victims of Sexual Abuse, Special-Needs, At-Risk Youth
12:30 – 1:15pm	Lunch, music, PIP, commentary, networking
1:15 – 1:45pm	Barbara Coloroso—Why They Cyberbully
1:45 – 2:30pm	Panel: Approaches – Education, Legal Intervention, Raising Awareness, Cyberwellness, Digital Literacy, Support
2:30 – 3:30pm	Breakout Sessions 1-6 Each charged with exploring a different approach and identifying when they are effective
3:30 – 3:45pm	Break and commentary, pics
3:45 – 4:00pm	Mustafa Ahmed—Spoken Word Performance
4:00 – 5:15pm	Closing Panel – Thinking about Justice and Taking it to Dublin

Programs and Speakers subject to change.

Panel One: Understanding Cyberbullying - The Different Kinds of Cyberbullying, How It Works, Who Does It, When Actions Cross the Line and Weaponizing Digital Technology



The 5 Types of Cyberbullies

1. The “Vengeful Angel”
2. The “Power-Hungry” Cyberbully
3. The “Revenge of the Nerds” Cyberbully (actually a sub-type of Power-Hungry that only happens online)
4. The “Mean Girls” Cyberbully
5. The “Inadvertent Cyberbully” (sometimes called the “Accidental Cyberbully”)

Understanding Cyberbullying Motives

“The Vengeful Angel” (Cyberbully

In this type of cyberbullying, the cyberbully doesn’t see themselves as a bully at all. They see themselves as righting wrongs, or protecting themselves or others from the “bad guy” they are now victimizing. They believe they are the Rob in Hoods of cyberspace. Vengeful Angels may be angry at something the cyberbully (or offline bully) did and feel they are taking warranted revenge or teaching the other a lesson. The Vengeful Angel cyberbully often gets involved trying to protect a friend or another student whom is being bullied or cyberbullied. When Vengeful Angels arise in a school, it is usually a sign that something in the system isn’t working. They step in because no one else does.

The “Power-Hungry” Cyberbully:

Just as their schoolyard counterparts, some cyberbullies want to exert their authority, show that they are powerful enough to make others do what they want and some want to control others with fear. Sometimes the student wants to hurt another student. Sometimes they just don’t like the other student, are just seeking a reaction or are just targeting the next person to log on (the classic wrong place at the wrong time motive). They are looking for attention and want to see their target(s) sweat. These are no different than the offline tough schoolyard bullies, except for their use of technology. And in most cases, they are the schoolyard thugs that use offline intimidation and their fists to hurt and control others and this is just another method of attack.

Understanding Cyberbullying Motives Cont'd

A sub-type profile of the "Power-Hungry" is called "Revenge of the Nerds." This type of cyberbully is often the victim of typical offline bullying. They may be female, or physically smaller, the ones picked on for not being popular enough, or cool enough (the "girls and the geeks"). They may have greater technical skills, as well.

They use technology to level the playing field between the strong and the weaker but tech-skilled. It is their intention to frighten or embarrass their victims in the same way as their beefier Power-Hungry cyberbully counterparts. And they are empowered by the anonymity of the Internet and digital communications and the fact that they never have to confront their victim in real life and risk being physically hurt. They may act tough online, but are not tough in real life. They are often not a bully but "just playing one on TV."

"Mean Girls" Cyberbully:

This type of cyberbullying is always mean, but not always committed by girls. It is a group sport and occurs when the cyberbully is bored or looking for entertainment. It is a social - exclusion method, where the cyberbully or teams of cyberbullies are showing their social clout. It is largely ego-based and they are the most immature of all cyberbullying types.

This style of cyberbullying is used more often by girls to harass others girls than any other type of cyberbullying. (Boys most often use a Power-Hungry or hacking attacks tactic.) It is used often for cross-gender cyberbullying as well and spreads very quickly. Mean Girls cyberbullying is often a campaign, rather than a one -off incident.

Mean Girl cyberbullies can do serious damage, especially to young teens and older preteens. In each case of teen cyberbullying -related suicide, the cyberbullies used "Mean Girl" tactics to harass their targets.

"The Inadvertent Cyberbully":

Inadvertent cyberbullies usually don' t mean to be cyberbullies at all. They didn't mean to hurt anyone but were just careless. Parry calls this category of cyberbully "careless and clueless." She sometimes calls them the "accidental cyberbully" too, since students have problems spelling "inadvertent." :-) They are the one exception to the "cyberbullying requires intent" rule. They are always surprised when others think they are cyberbullies.

Often Inadvertant Cyberbullies leave out crucial words when typing and are not careful about what and how they say things. The recipient doesn't understand that the hurt was unintentional. That's why it is still considered cyberbullying.

Inadvertent cyberbullies may be reacting to hateful or provocative messages they have received. Unlike the "Revenge of the Nerds" cyberbullies, they don't lash out intentionally. They just respond without thinking about the consequences of their actions. They don't think before clicking "send."

They might have been kidding around and their jokes not appreciated, or may have used a new screen name that the "target" doesn't recognize. And maybe they just sent a message to the wrong person and that person takes offense.

Why Do Young People Cyberbullying Each Other?

Cyberbullying is often motivated by anger, revenge or frustration. Sometimes cyberbullying is entertainment , when they are bored and have too much time on their hands and too many tech toys available to them. Many do it for laughs or to get a reaction. They may do it because they think it's fun. And a growing number do it to make a point to others, to improve their ratings, popularity or video's page views. They are looking for attention and their "15 megabytes of fame."

The Power-Hungry cyberbullies do it to intimidate and control others. They want to be in charge.

Revenge of the Nerd cyberbullies (a sub-type of Power-Hungry cyberbullies) may start out defending themselves from traditional bullying only to find that they enjoy being the tough guy or gal.

Mean Girl cyberbullies do it to help bolster or remind people of their own social standing.

Vengeful Angel cyberbullies think they are righting wrongs and standing up for others.

Inadvertent cyberbullies never meant to hurt anyone. They did it by accident.

Activity: Come up with two examples of why young people cyberbully each other and what could have been done to prevent it.

Who is a Typical Cyberbullying Target?

Any child, preteen or teen is a potential cyberbullying target. They don't need to have home Internet access, a cell phone or any cyber -connection. The cyberbullies are perfectly happy to have the technology do their dirty work in destroying reputations or creating offline responses to online provocation. Obviously, when friends have a falling out or romance takes a bad turn, cyberbullying is a viable option to settle scores and share hurt feelings. According to Teenangels' research and surveys, 70% of cyberbullying comes from friends or acquaintances.

Bigotry, hate and intolerance are big motivators, as well. Anyone who has been the target of offline bullying or is more vulnerable to it is a likely target too. Jealousy plays a powerful role in motivating cyberattacks by those involved or formerly involved in relationships, or those rebuffed by the ones they like. Friends pile on fast to "defend" their friends' honor, and lines are drawn in cyberspace.

The more a student shares personal and private information, gets involved in heated online debates or has an offline problem, the more likely they are to be targeted. Vulnerable students are often targeted because it's so easy to target them. Maybe there is something going on at home– a divorce, a serious illness of death in the family, a financial crisis that make them especially vulnerable. Cyberbullies can sense that and use it to their advantage. Special-needs students, newcomers and immigrants, victims of assault and students whose intimate images have been shared with others are often the most hurt by cyberbullying and the first to be targeted.

Cyberbullying targets popular students too. Those who are jealous of their popularity or envy their status will use digital bullying methods to target them, without letting anyone know who they are. They see it as taking on the entitled and popular kids to make things "fair" for everyone.

Digital Hygiene and Digital Self-Defense

Digital hygiene isn't about electric toothbrushes and flossing devices. :-) It's about keeping your digital devices, accounts, personal information, files and access secure. You do that by using good security practices, using the right passwords and keeping them private and keeping an eye on your reputation online and off. Think of digital hygiene as digital self-defense. Most digital problems can be avoided if you prepare in advance. It is much harder to stop cyberabuse once it has begun than to prevent it in the first place.

Keeping Your Devices Clean

An important part of digital hygiene is keeping your computer and other devices "clean." That means avoiding spyware and other malware (such as viruses and other applications designed to harm your devices or data). (Staysafeonline.org coined the term "keeping a clean machine" to describe this.)

Spyware and malware can be installed on your device in several ways. The most common are by clicking on a link, sharing a flash drive or storage device, or downloading or accepting a digital file. Malware is designed to harm your device or data. Spyware is used to "spy" on you, your files and what you do with your device. Some spyware can even give others access to your device by remote control.

Luckily, it's easy to avoid spyware and malware if you are careful and think ahead. Most good security program offered by well-known security software providers will help spot and remove most spyware, keep others out of your devices and files and prescreen for malware. Just make sure they are correctly configured and set to update automatically to keep you and your devices protected. Most work you're your computer, but some also protect your mobile devices from spyware and viruses.

Just as important as keeping a clean machine is locking your devices, accounts and files. This involves the use of the right passwords and selecting the right privacy and security settings. Password theft or abuse are often the root of digital problem. They are easy to guess, hard to remember, stored on a device or shared with others. WiredSafety.org's studies have shown that most teens share their password with at least one other person (typically their boyfriend/girlfriend or best friend) and often adults do too. And we rarely use different passwords for different sites or purposes, which means once someone has it for one network, they have it for all networks.

Remember that giving your password out is like locking your door, but giving someone the key and burglar alarm code. It's not very smart. Make it a hard and fast rule never to share their passwords.

Too many computer and account intrusions arise just because the password was easy to guess (such as the word "password," or "12345") or because it was one of the "20 questions" used to come up with most passwords (such as our pet's name, our middle name, the street we live on, birthdate or anniversary, the year we graduated or will graduate high school, favorite sports team or rock star).

Use passwords to lock your devices when not in use, as well, and to protect certain sensitive files, folders and features. And, on Facebook, consider authenticating your device, by letting Facebook know which devices you use. This prevents your account from being accessed by someone else from a different device. It's a fast and easy way to avoid major problems.

We should also learn about privacy and access choices available for our favorite networks. We can restrict certain specific people or, in some cases, everyone except our friends from contacting us or being

able to view our posts. Once we make their choices, we can enforce them using privacy, security and personal settings provided by the device manufacturer, service provider or network.

ThinkB4uClick

We send tons of texts at the same time we are talking to friends in real life. It's understandable that we will end up sending a message to the wrong person by accident, or leave out words or emoticons (like smileys or frownies) that let them know what we really meant. A misunderstood message or a message in the wrong hands can lead to a cyber world-war-three.

Try and slow down long enough to reread what you are planning to send. Did you send it to the right person? Did you leave out an important word that changes the meaning? Will they understand what you meant? If not, take a second longer and make it right. Think about the person on the other side. Is what you are sending hurtful or sarcastic? Do they understand enough about the context of the message to understand it? Should you be using a different medium for the message? Some messages are better delivered in person (like breaking up), others can be done better by phone (complicated discussions) and some are just fine in texts and IMs (quick updates, sending a phone number, address or schedule). Some are public, some are more private. You should decide which is better in each case. The StopCyberbullying Toolkit has resources on selecting "the right medium for the message" and is available without charge to schools at StopCyberbullying.org.

Act Fast

If you and your romantic partner break up, before you cry yourself to sleep or check the dating ads, change your password. If you get into a fight with your best friend turned enemy, change your password. Make sure you choose one that is easy to remember but hard to guess. The faster you act to lock out others from your accounts and groups, the better.

If you see cyberbullying, report it right away. Many huge cyberbullying campaigns could have been avoided if Facebook and other social networks knew about it early enough. The longer you wait, the faster it grows. Received a "sext"? Delete it. Do not pass it along, copy it, save it or print it. Get rid of it as fast as you can. Possession of child pornography is a serious crime. If the pic is of someone under the age of 18, in the US you can be charged as a sex offender for just having copies of these images on their device or online storage accounts. If you took a sext image, think before saving it or sharing it. The faster you engage your brain cells the safer you'll be. Delete it from your phone and destroy all digital or printed copies. Someone can easily grab your phone when you're not looking and broadcast it to everyone or send it to them to hurt you later.

Keeping an Eye Out

Facebook, Google, Bing , Twitter, Instagram and Yahoo! yourself. Search for your whole name (in quotes to search as a phrase). Search for your cell number, screen names and email addresses. Search for your nicknames and home address. Then set an "alert." Alerts send you a message any time the search engine finds this information online. The faster you know about something that is posted about you that shouldn't be, the faster you can do something about it.

Some posts on social networks don't get picked up by search engines, so double checking there can help. Consider it an early warning system. While you're at it, keep any eye out to protect your friends and family members too.

Bystanders in Cyberbullying

"Bystanders" are people who witness actions. In cyberbullying cases they may receive a copy of the cyberbullying message, be asked to vote for the "ugliest girl in school," view a cyberbullying attack on someone's Facebook, be a friend of the victim or cyberbullying or hear about an upcoming cyberattack.

Sometimes bystanders are active, such as when they forward a mean message, or pass along the url of a YouTube harassing video about someone. Sometimes they are passive, such as when they know about the cyberbullying, might have stumbled on a harassing profile or have received a copy of the message without forwarding it on.

When cyberbullying is involved, Parry Aftab calls active bystanders "Facilitators." Most large cyberbullying campaigns won't get very far without the assistance of Facilitators. They are used as the grease to speed up the wheels of the cyberbullying campaign – to drive attention to what's going on and to keep it going. Without Facilitators, most cyberbullying campaigns fall flat. It's like hosting a big party when no one comes. Mean girls rely on Facilitators to help them do their dirty work. Sextbullying couldn't happen without them.

They do more than merely observe the cyberbullying. They instigate further abuse and create the buzz that every good digital campaign needs. They pass along the messages, embarrassing photos and promote others to join in. They may pretend they aren't involved, but their activities are essential to spreading the abuse online. Facilitators can do this intentionally or be manipulated by the abuser into believing that the victim is in the wrong and serves whatever is happening to them, another example of "cyberbullying-by-proxy. (Read about "Dupes" below.)

The more active they are, the bigger part of the problem they become. They become the vehicle for the cyberbullying when they gladly pass along mean messages written by the original cyberbully. Sometimes the Facilitators become cyberbullies themselves. When their actions are more than just "spreading the news" and they become more active by voting for the "ugliest girl" in the mean quiz or for escalating the cyberbullying by adding additional inflammatory facts or rumors they have gone from Facilitator to active cyberbully.

Dealing with Facilitators requires someone to "step in or step up." Like throwing water on two fighting dogs to get them to "cool down," someone needs to throw some cold water on the Facilitators' actions. This can be a third party ("stepping in") to try and get people to stop the mob behavior or gain perspective. Or it can be someone "stepping up" from the group of Facilitators or passive bystanders to convince everyone to stop.

Most teens are afraid to get involved, fearing that they might become the next victim. This is especially the case when offline bullies, power hungry cyberbullies or mean girl cyberbullies are involved. Using the dog fight example, stepping into the middle of a wild dog fight will risk a serious bite or the dogs turning on you. If you step into a cyberbullying situation without being prepared, you can get hurt just as easily. (Read the article "Step In or Step Up! How to help stop cyberbullying." It can be found on StopCyberbullying.org or in the StopCyberbullying Toolkit, in the Resources section.)

Passive bystanders need to recognize when they should do or say something. They have to be taught to identify cyberbullying when they see it, and when to report cyberbullying to the school, parents, the

Bystanders in Cyberbullying Cont'd

website or to the police. (This applies even more to digital dating abuse.) They need to know how to report abuses on the sites they frequent and understand the report abuse process.

Often teens are unwilling to report cyberbullying when they encounter it with themselves or with others. They have a cultural reluctance to tell adults about anything, fearing it makes them look immature or that they could be seen as tattling. They also worry that if they are wrong and it wasn't really cyberbullying (perhaps just an inside joke) they might get into trouble for making a false report. They worry that the person they are reporting might be told who reported them (they aren't) and worry about retaliation. (You can learn more about this in Step In and Step Up!) What they need to worry about more is the hurt someone is experiencing that they may be able to help stop.

Friends, whether they are best friends or just classmates, neighbors or someone you've known since 2nd grade, have a higher obligation than mere bystanders. They know and should care about you. They are supposed to be supportive and stand by you when you need it. Yet, often friend- bystanders try to avoid getting involved, fearing that the cyberbully will turn on them or that they will somehow get into trouble. So, they often opt to do nothing. They sit by and watch someone they care about get hurt.

Friends don't always have to report the cyberbullying. They may decide, after talking with their friend who is being targeted, that reporting it is not the best way to handle that case of cyberbullying. The best thing they can do is stand by and be supportive of their friend. They need to understand how to be supportive of someone they care about too. (Ask the person what they would like you to do or not do. It's a good place to start!)

Whatever they decide to do, they have to do something. Martin Luther King, Jr. once said "In the end, we will remember not the words of our enemies, but the silence of our friends." Don't be remembered for your silence.

There are two significant additional types of digital bystanders – 1. strangers who witness the cyberbullying online and know neither the victim nor the cyberbully and 2. "cybermobs," "flamers" or "trolls" and "dupes."

Cyberbullying usually occurs among people who know each other offline. They are armed with secrets, often with passwords (or can guess them easily) and have a stake in the harassment. They may have been harassed by the victim previously, or believe that the victim "deserves it." They may be angry, vindictive or jealous. They are often seeking an audience of people who know both them and the victim. And they typically try and fuel the cyberbullying fire by getting others to join in.

But because of the nature of online social communities with 1 billion+ users, it is inevitable that strangers will witness cyberbullying that is posted online or send in viral messages. For example, sexting-related harassment can result in tens of thousands of strangers viewing the nude photo. As a young teen once explained, "In the beginning it's a shocking picture of someone you know. You have a stake in protecting her or sharing it with others because of who she is. But as it continues to move outside of your school and community, it eventually just becomes a picture of some naked girl."

Those who receive or view that picture "of some naked girl" are strangers witnessing sextbullying. They

can report it, ignore it, delete it or pass it on. And their choice can make a significant difference in the duration and scope of the sextbullying. And, to the victim trying to contain the harassment, it can make all the difference in the world. Empowering bystanders to report what they see is crucial.

Defining Cyberbullying-Related Terms

The definitions of the different terms are set forth below and on the "Cyberbullying Terms" glossary provided at StopCyberbullying.org and in the StopCyberbullying Toolkit, in the Resources section.

"**Cybermobs," "Flamers," and "Trolls":**

"Cybermobs" don't know or care who the victim is, feeding on the vulnerability of the victim. There may be strategic positioning of the digital abuse to make the victim appear to be the bad guy. These often involve cyberbullying-by-proxy staging when someone manipulates others into doing their dirty work for them, causing those third parties to believe their actions are righteous and that they are seeking justice. The victim is re-victimized as the focus of their mean comments and vicious attacks. The only way, generally, to stop a cybermob is to wait it out. The best way to address it is to prevent it from happening in the first place or stopping it very early in its evolution before it takes on a life of its own.

"**Flamers" and "flaming":** nasty comments, insults and rude communications posted online for various purposes, including anyone holding opposing opinions or doing things they don't approve. "Flamers" tend to act alone in their attacks and are highly opinionated, attacking anyone with other opinions or if they find them offensive in any way.

"Trolls": are people who like to stir up trouble online and see what happens. A juicy rumor campaign can "feed the trolls," allowing them to act out and giving them the attention they crave, especially in virtual worlds and interactive games.

"Dupes": are people who engage in harassment or cyberbullying activities after being convinced that they are doing the right thing, giving someone something they deserve or believe that the person they are targeting started it by harassing them first. The person is being manipulated by the real cyberbully into falling for this. It's a cyberbullying-by-proxy campaign designed to get others to do their dirty work and the dupes fall for it.

"Cyberbullying" is "any cyber-communication or publication posted or sent by a minor using any digital technology that is intended, directly or indirectly, to frighten, embarrass, pose as, harass, hurt, set up, cause harm to, extort , intimidate or otherwise target another minor."

A shorter definition: "Cyberbullying" is when minors use technology as a weapon to intentionally target and hurt another minor." And the shorter definition works pretty well. With one exception, all cyberbullying must be intentional. It requires that the cyberbully intends to do harm to or annoy their target. (In the one exception to this rule, "inadvertent cyberbullying," the target feels victimized, even if it is not the other student's intention. Since it often leads to retaliation, traditional cyberbullying and cyber warfare, it is considered one of the five main types of cyberbullying.)

Cyberbullying needs to have minors on both sides, as target and as cyberbully. (If there aren't minors on both sides of the communication, it is considered "cyber - harassment," not "cyberbullying.") When a student harasses a teacher, it falls under cyberharassment, not cyberbullying.

Breakout Session One: We can't stop cyberbullying until we understand it. There are different methods used by cyberbullies. Each kind of cyberbully falls into a special profile. And cyberbullying works in different ways. By understanding how these work, we can start seeing patterns. And with patterns, we can start framing solutions. We also need to understand the difference between a rude comment, a serious threat, reputational attacks, someone posing as you to get others to attack you and a mistake or accident where someone forgot the include a word or sent the message to the wrong person. We need to define cyberbullying to stop it.

How do you define "cyberbullying"? Minor to Minors, Using Digital Technology as a Weapon to Hurt Someone, Repeated Actions for Lesser Attacks or a One-Time Serious Attack, Directed at an Individual or Group of Individuals, Intentional, the Target and Cyberbully Know Each Other. What else?

_____

Mean, Mistakes, Jokes and Cyberbullying. Telling the difference and understanding the risks.

_____

_____

_____

Understanding different cyberbullying methods and how devices are abused to cyberbully.

_____

_____

_____

_____

Defining the five categories of cyberbullies.

_____

_____

_____

_____

Defining the four different kinds of cyberbullying.

Direct:

_____

Indirect:

_____

Cyberbullying-by-Proxy:

_____

Privacy Invasions:

_____

Crossing the line and knowing where the line is. (see special worksheet)

Defending Yourself:

_____

_____

Telling the Difference Between
Mean Messages, Mistakes and Cyberbullying.
Above, On and Below the Line!

Cyberbullying!

1. _____
2. _____
3. _____
4. _____
5. _____

Sometimes These Things are Cyberbullying and Sometimes They Aren't. It Depends.

1. _____
2. _____
3. _____

Mean, Hurtful, Rude
(but not cyberbullying)

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____

What did I learn?

_____
_____
_____
_____

What questions do I have?
What do I want to share?

Change the world one post at a time!

postitpositive.org

POSTit positive

Facebook.com/postitpositive
Twitter: @postitpositive

POSTitPositive is a new program designed by an 8 year old to help other young people learn to post positive things online. She wants everyone to use digital technology to make others feel better about themselves.

Roisin lives in Prince Edward Island, Canada. She attended Parry Aftab's last StopCyberbullying Youth Summit and was sad when she learned how mean some people can be online to others. She thought that by using PostIt notes, kids who were too young for Facebook could practice posting by writing things on the sticky sheets and sharing them with friends in real life.

When she told her classmates about it, they all wanted to help. And with the help of her family, Roisin covered a big wooden lighthouse with PostIt sheets and pictures of POSTitPositive messages sent to her from all around the world.

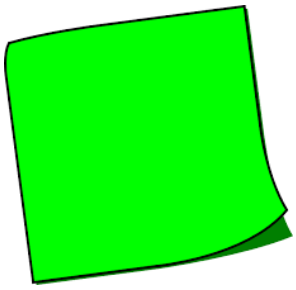
She always wanted to visit Ireland, the home of her ancestors. She always wanted to fly in a jet plane too! Now she can hare POSTitPositive while visiting Ireland on a giant plane! She really wanted to meet lots of Irish children and teens and see Adare Manor and Dromoland Castle.

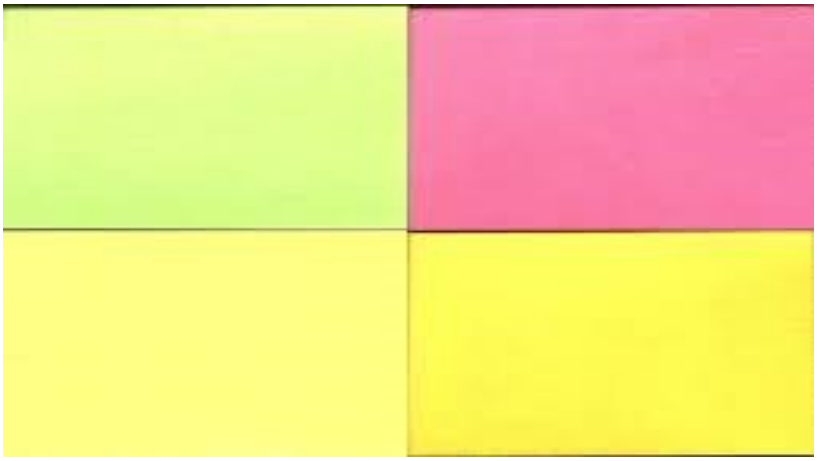
Now with the help of her mom and dad, Roisin is launching Postitpositive.org. Visit and say something positive. Ask others to sign your POSTitPositive pages at the Global StopCyberbullying Youth Summit 2015-Ireland.

And remember—You can change the world one post at a time!

My POSTitPositive Notes

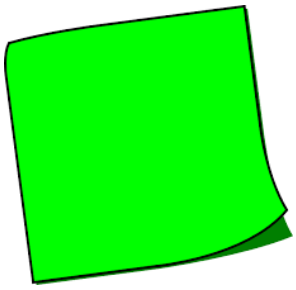
I am changing the world one post at a time!

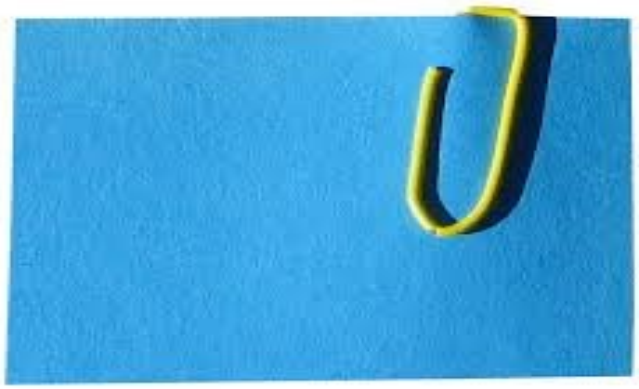


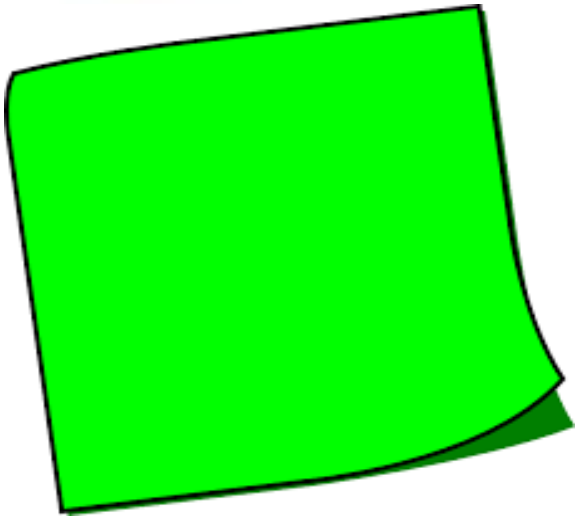


My POSTitPositive Notes

I am changing the world one post at a time!

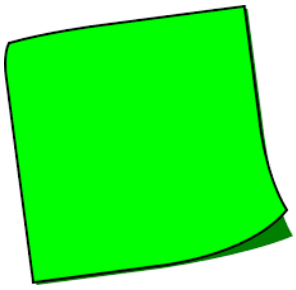


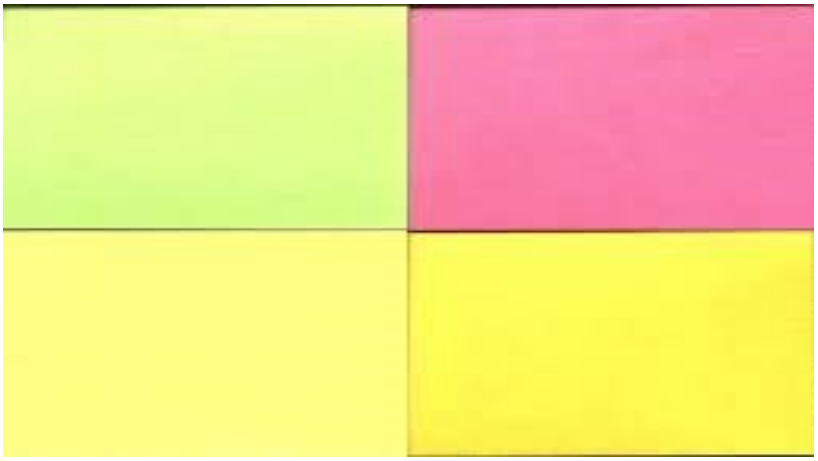




My POSTitPositive Notes

I am changing the world one post at a time!





Defining Your Terms:

You will hear lots of new terms over the course of the Global StopCyberbullying Youth Summit. Keep track of these new terms by writing them and their definitions here:

New Term: _____

Definition: _____

New Term: _____

Definition: _____

New Term: _____

Definition: _____

New Term: _____

Definition: _____

New Term: _____

Definition: _____

New Term: _____

Definition: _____

New Term: _____

Definition: _____

New Term: _____

Definition: _____

New Term: _____

Definition: _____

New Term: _____

Definition: _____

New Term: _____

Definition: _____

New Term: _____

Definition: _____

Best New Terms:

_____

_____

_____

_____

_____

WiredSafety.org's Teen Cybersafety Guide

I know. You're sick and tired of being lectured to. You know how to keep yourself safe online. You're not a baby! You use privacy settings on Facebook and Instagram. You don't say things you will regret on Twitter or Ask.fm. You aren't meeting "strangers" offline. You are careful. You aren't sharing too much info and you think the media has blown the risks out of proportion. You keep your clothes on in pics and don't send death threats to your teachers.

Great. You can stop reading now and go have fun doing something else. For the rest of you, just in case there is something you hadn't thought about, or you have a friend who isn't as careful and smart as you are...

Don't Be Stupid!

Most teens understand enough about cybersafety to write a book. They don't want to be hurt or get into trouble. The problems that WiredSafety are seeing when teens are connected through cell phones, game devices or the Internet itself are either because the teen didn't know enough about the technology, or because they were just "being stupid" and not thinking.

Stupid is when you decide to pose nude for a cell phone photo or webcam video for any reason. Stupid is when you believe your boyfriend when he tells you he would never share the photo with anyone and no one else will see it. (Even if he is trustworthy, he might have a little brother who isn't, a friend using his cell or a parent who checks his cell phones once in a while.)

Stupid is when you think no one can figure out that the anonymous email, post or profile you made came from you. (They collect the electronic footprint when you interact online that can be traced back to your computer or cell.)

Stupid is when you do things online that you would never do offline just because you can.

Stupid is when you think that cute sixteen year old boy or girl you met online is always a cute sixteen year old boy or girl.

Stupid is when you think someone will send you an iPod just for playing a game and giving them some "harmless" personal information (like your dad's credit card number).

Stupid is when you know better, but do it anyway.

There is something about the technology that makes you think that the people who are reading your posts or blogs are only the ones you want to read them. You talk to them. You post pics and videos for them. You are funny for them. But sometimes "they" include others who would love to harass you, get you back for something or are just plain old creeps.

And when you are typing as fast as you do, you leave out words or letters, think something is clear when it's not or even send it to the wrong person. When you make these mistakes, the person who receives it may not know that you weren't trying to freak them out. And they may react as though they were harassed or threatened. That's when you get reported to Facebook or the police, or the target of

an “Oh, yeah? Well you started it,” campaign.

Okay, Already. You Told Me What I Can’t Do. What CAN I Do?

Teens tell Parry Aftab (a cyberlawyer who is also the founder of WiredSafety) and her Teenangels (Teenangels.org) that they know what not to do already. They want to know what they can do. So here goes.

You can post a picture online. Just make sure it’s one your parents, principal, a predator and the police can see without you getting hurt. And for good measure, add in prospective college recruiters and employers and the (future) love of your life too. And the picture you post should be your own. If others are in it, ask first. It’s common courtesy and hopefully will be reciprocated when they are thinking about posting that picture of the two of you when you were 11 that you thought (and desperately hoped) was deleted long ago!

And be careful what you tag. Every tag identifying you in a pic is a potential sharing of too much information. A picture can say a thousand words and in cases where the pics are tagged and circulated, can come back and haunt you. Tagging makes it easier for college recruiters to see what you really do, instead of what you said on your application you do. Your parents might see you drinking at a party. Or when you were somewhere you weren’t supposed to be at that time, you are outed big time.

You can have a Facebook (or other social networking) profile and still be safe. It just requires that you are choosy. You have to be choosy about who can see it and what they can see. (Visit Facebook.com/privacy and understand your privacy choices.) You can decide that one friend can see everything, but another one can’t see some pics. You have to be choosy about the site itself. Who else is on that site and what kind of an impression does the site make? Fun? Freaky? Wild? Slimy?

Choosing your social networks is like choosing where you want to live. Remember who your neighbors will be.

You should also delete old profiles you are no longer using. It’s pretty easy if you know your login and password. But if you forgot the login and password, or aren’t using the same email address you had in sixth grade when you set it up, it can be harder. Ask the network for help if you need it. Most have a procedure to shut down old profiles and prove they are yours.

You can talk to online “strangers” safely too. We know that parents will freak if they read this one. They have warned you since you were three to avoid “strangers.” Then “strangers” were creepy men in black raincoats who hadn’t shaved in weeks. Now “strangers” are people you don’t know in real life that you have met online.

Think of it this way. If you were on a bus with your mother when you were five and an old lady sitting across the aisle compliments you on your shoes, would you run screaming from the bus? She’s a “stranger” right? But she wasn’t threatening, creepy or inappropriate. At the same time, your mother would not have whipped out her wallet and told the old lady where she bought them and that she paid for them with her VISA card and given the old lady the account info.

It’s not talking to strangers that is the problem. It’s what you talk about. This works online and offline. If you meet someone online from Australia, it would be interesting to find out what an Australian teen does for fun. Do they all have pet kangaroos? And they would have similar questions about

teens from Texas. Do they all ride horses to school? And maybe they will have less boring things to share too. :-)

When communicating with new people online that you don't know in real life, remember the bus story. No credit card information and nothing you wouldn't tell a stranger on a long bus ride. And remember:

- They are not your "friends" just people you met online.
- They shouldn't get information you wouldn't give to an offline stranger.
- And that cute sixteen year old boy (or girl) you met online may not be cute, may not be sixteen and may not be a boy (or girl).

How can you be safer when meeting online friends offline?

There's no way to be entirely safe when you meet people in real life, period! And while we will tell you never to meet them in real life, some of you will ignore us and meet them anyway. The idea is to get you back safely, if you do.

So, if you are going to ignore our advice about meeting people offline, you can stay safer as long as you remember:

- Go as a group. (Parry suggests bringing some sumo-wrestlers with you too. J) They can always give you some privacy later once the person is who they said they were. Even consider bringing a parent (if they are cool parents).
- Meet in a very public place, but not a noisy one like an amusement park, where no one can hear you shout.
- Have an exit strategy. If you decide this was a bad idea, have a plan for leaving safely and quickly.
- Start out by telling them before you meet that your parents are waiting for you in the Mall (or wher-ever you are meeting) and you won't have much time. You can change that if you feel comfortable.
- Have realistic expectations. Remember that everyone lies a little, so be prepared and make sure you only lied a little.
- Take things very slowly. You may think you know and can trust them, but you only know what they said, not necessarily who they are inside.
- Give yourself time to get to know them in real life before taking it any further. You don't owe them anything!
- Trust your gut. If things feel wrong – get out of there right away. Don't worry about hurting their feelings.
- And if it's a creep, not the person you thought you were meeting, report them. Even though your parents might find out and be very unhappy, you might be helping protect the next potential victim.

Now, for what you *should* do:

ThinkB4uClick

Suggesting that any teen slow down and proofread their texts or IMs is probably a waste of time. But taking a second to decide if you really want to send that or whether you will regret posting something is

a good idea. The only time you can protect yourself from the consequences of things going wrong is BEFORE you click the “send” button.

What you post online stays online – forever! (One of Parry’s favorite lines, but true.) Deleting it afterwards may not delete it from everyone else’s copies, Google or what was already printed out, forwarded or saved.

Use privacy settings on all your profiles and photo and video-sharing pages.

You want to decide who can see what. But always remember, while you may restrict your Facebook to the group for teens in your high school, most groups have people in them who don’t belong there, starting with teachers and school administrators and coaches. Assume they are reading your stuff too when you post to a group.

Respect yourself and others

It’s a boring message, but probably the most important one we can share. Put yourself in a mental time machine and fast forward to when you are 30 years old. What will you be doing with your life? Who will be important people in your life then? Now look at your profiles and online posts, pics and videos. Is there anything there that you wish (as a 30 year old) you could erase? The time to do it is now, before it affects your future. What seemed like a good idea at the time, especially if you had a beer or two at a party, may not be when you wake up in the morning. And don’t do anything online that you wouldn’t do offline – that’s the Internet Golden Rule.

Choose a password that is easy to remember but hard to guess.

Most teens (and adults) choose passwords based on “20 Questions.” They use the same 20 questions to come up with their passwords, like their middle name, their pet’s name, their birth date, the town they live in, their favorite movie, their best friend’s name, the car they want to drive, the year they graduate, the college they want to attend, etc. The problem is that these are pretty easy to guess when you know someone pretty well. Just think about how many of these you could answer about your friends and others in your class. And if you can guess theirs, they can probably guess yours too, unless you are careful.

Lots of security experts tell you to use a password with upper and lower case letters, numbers and symbols. That might be good for security experts, but it’s really hard to remember. So, you have to write it down and stick it on a post-it sheet on your monitor to remember. How secure is that? Not very!

Instead, use a sentence with a number in it. You start it with a capital letter and end it with punctuation (a symbol!). Upper case, lower case, numbers and a symbol. Easy to remember and hard to guess. Just make sure you aren’t using your favorite quote or something you have posted on your Facebook page.

Teenangels (teen Internet safety experts at teenangels.org) tell other teens to use a different password for each site. You can use the site name in the sentence and it’s different for each site and secure, as well as easy to remember. “Facebook has more than 1 billion users!” Wow! (And it’s a pretty good password once you leave out the spaces.)

Or choose something only you would know, that is easy for you to remember and no one else can guess (even and especially your "BFF"). Choose your favorite character in a book and how old you were when you first read that book, or the best birthday resent you ever got and how old you were when you got it. That gives you numbers and letters and is easy for you to remember, but hard for others to guess. Get it?

More than 70% of teens polled said that they had shared their passwords with at least one friend (often their boyfriend or girlfriend). That's one friend too many, especially when friends get into fights or couples breakup. It's not smart since, when armed with your secrets and your passwords, friends can do some serious damage.

It's also not a good idea to click "save my login and password" when using a computer that anyone else can access, like your little brother or sister, your friend's computer or one at school. Let your friends know that friends don't ask for their friend's passwords. Find another way to show them how much you trust them.

Cyberharassment, Cyberstalking and Cyberbullying

Teens say that "cyberbullying" is sooo "primary school." They are too mature to do those kinds of things in secondary school. Think again! While it might be called cyberharassment instead (if they are eighteen or over), or might not even have a name in secondary school, when people take over your accounts, pass nasty rumors, have a quiz on how ugly, fat or stupid you are...they are cyberbullying you. Cyberbullying is when one minor uses technology as a weapon to hurt another minor. Whether they are passing around a nude pic of the victim to embarrass her, or sending around texts lying about what she said or did, or reprogramming his cell phone, it's cyberbullying.

When they steal or misuse your password and pretend to be you online, it's cyberbullying. So, call it what you want, teens still use technology to hurt each other all the time. Often offline bullies start this stuff. But sometimes you start it when you overreact to something someone else did or said. "They started it" doesn't matter.

The best way to handle any harassing message you may receive is to "stop, block and tell!" You should stop and not answer back. It only feeds the harassment campaign. You should block the person or message. Why torment yourself further or give them access to you? And you should tell someone you trust, preferably an adult. Teens have committed suicide when cyberbullying gets out of control. Talking to someone can help you keep things in perspective. Using an adult to confide in means you are never confiding (without knowing it) in the cyberbully. (Seventy percent of cyberbullying occurs anonymously, so you never know if it's your best friend or worst enemy. But you know for sure it's not your teacher, guidance counselor or your parents.)

And if you are tempted to answer back...do something else. Parry Aftab and Teenangels call this "Take 5!" Do something you love to do for five minutes to help you calm down. Just make sure it doesn't involve a cell phone, computer game device or computer, so you won't do something you will regret later.

Cyber-Romance

You're bored, it's Saturday night and he has a great pic on his Facebook. You are finding love in all the cyberplaces. But how safe is it to flirt online, or meet someone in real life that you only know online?

Before we begin, remember that "flirting" doesn't mean taking off your clothes for the camera. You should already know that's just plain stupid. Flirting should also not involve "cybering," ("Cybering is like phone sex, but typed.) since that can come back and haunt you. Be funny. Be interesting. Be gorgeous or an athlete. Be smart.

Talk about things that you won't regret later on. Don't share secrets. Then if you want to take it further, move to a webcam or the phone. (Block caller ID though and remember that they could be recording the cam chat.) Take it slow. And check them out. Visit their school website or Facebook group and see if you can find them there.

Check any other personal details they have provided too. If enough time has gone by and s/he is consistent, hasn't been lying (to your knowledge) and checks out, you can consider meeting them face to face. But you'll need to follow the safer meeting rules above. And remember, the only thing hurt is your reputation if something goes wrong online. But teens have really been killed by someone they agreed to meet in real life, after only knowing them online. So, think twice, three times...be careful.

Sexting

Sexting uses cell phones or other technologies to take nude or sexual images and share them with one or more people through text messages, video-streaming or online posts. Although using texts and cell phones to take and share the pics is new, similar activities have been going on since before you were born. People your parents age used to take these kind of pics with Polaroid cameras (which spit out instant hardcopy pics).The first digital sexting case Parry encountered was in 1998, where a teen girl took videos of herself to give to a boy she liked. He shared that video with everyone online! (And didn't ask her out either.)

All teens know it's not smart to do this. But many do it anyway. They do it because they are in love. They do it because their boyfriend begs them to do it. They do it when they are bored, desperate, drunk, high, at a slumber-party or just plain stupid. They do it when they like someone and want to get their attention fast. They do it to impress others with how sexy or well-endowed they are or as a "look at what you are missing" message. Younger teens and preteens do it to attract older boys or because they think it makes them more "mature." The point is not why they do it. The point is what happens afterwards.

Jessie Logan, an eighteen year old high school senior from Ohio, took a nude picture and stored it on her cell. A girl she knew liked a boy who liked Jessie. You know the drill. The girl got access to Jessie's cell and texted the pic to everyone. Everyone in her town saw the picture. They called her names and were horrible to her. When no one tried to help her, she ended up taking her own life. And she is not alone. Many of you have seen the YouTube video of Amanda Todd, the teen from Canada who was blackmailed by a creep who had a topless pic of her. She ended up taking her own life, as did several others under similar situations.

While these are extreme cases and still very rare, the humiliation can be more than some teens can

handle. And the pics often end up in the hands of creeps who post and share them with other creeps. As in Amanda's case, many teens have been blackmailed into doing things they didn't want to do, because the blackmailer knew about or had a copy of one of those pics or videos.

And police and prosecutors around the world are now treating this as a serious sex crime. And in some countries, including the US, the teens involved are being charged too. Teens who have taken a nude picture of themselves are being charged across the US as child pornographers and are becoming registered sex offenders. Those who forward the pics are being charged with distribution of child pornography. And those who keep a copy are being charged with possession of child pornography. If you become a registered sex offender you can't live near a school or public park. Your college must be informed and so will your employers. You will be forever grouped with those creeps we try to avoid.

And try and explain that the reason you are a registered sex offender is because you took a nude pic of yourself and posted it on Instagram. Who will believe you? Everyone will think you molested a child.

These are real risks and happening to teens across the US right now. So if he tells you that you can prove you love him by taking a nude pic and sending it to him, tell him if he loved you, he wouldn't ask. And if she tells you that she needs a pic to "remember you by" promise her that all she needs to do to remember you is call or text.

Confiding in Strangers Online to Provide You with Important Advice

It's tempting to share secrets or search for places online where you can get advice on things you may not want to discuss with friends or even your parents. But what makes you think that a stranger in an online forum is smart enough to give good advice? And why would you post information in public that you wouldn't share with family or friends in private?

There are some very good places to visit online where experts can advise you on health, safety and personal matters. But you can't always tell which ones are trustworthy or which ones are crackpots posing as experts. Ask around. Ask your guidance counselor at school, or use a trustworthy resource to help you find one. You can start by looking for a .gov site (they are all run by governmental agencies). Or find a charity you know offline or have heard about in a magazine or on a TV show you trust.

Then use privacy settings, a special email address you create just for this and think carefully before you share. The best advice may come from people you trust who know you in real life. But online help can be there when you need it 24/7 and be anonymous too.

Who Knows More – Teens or Parents?

If we are talking about the Internet, the answer is obvious (even if your dad is Bill Gates). Teens know more about the Internet, at least the way they use it. They know more about cell phones and gaming devices too. But, like it or not, parents know more about life. The good thing is that you can both share what you know with each other pretty easily.

You should "have the talk" with them and let them know you won't do anything stupid, you care about staying safe and know what you need to know to do that. Show them your Facebook and Instagram profiles. (Whether you "friend" them or not is up to you and them.) Show them where you

spend most of your time online. Teach them how you search for things. Help them install and use security software.

And offer to help keep your siblings, nieces, nephews or cousins safer online. Help your parents set up their own Facebook or Instagram account. Show them how YouTube works. Teach them about privacy settings and remind them to check with you before posting any pics of you online.

Talk with them about what you want them to do to help you. Parry Aftab said “the best filter is the one between your ears.” Let your parents know you have a pretty powerful filter that’s called good judgment and strong values. Remind them that they can trust you and promise to come to them if anything goes wrong. They can’t help you if they don’t know you need help. You should never face things alone. That’s what families are for.

Now, have fun, be safe and don’t be stupid!

Bully listing

Likes to pick on others who are less fortunate or have physical differences. Enjoys getting together with friends and attacking others online for a laugh.
When she is done taunting she leaves a flower covered call card with the words "love me I'm beautiful", printed on it.

What he lacks in physical strength he makes up in brains. He likes flexing his "virtual muscles" by disrupting the workflow of his classmates and occasionally even the teachers.
His online callsign is VRMan and he's not afraid of anyone who posesses a computer.

She is a wanna be cheerleader but is always turned down during try-outs.
She enjoys time with her best friend Mittens (her cat), and taking the time to virtually attack those who she sees as a tyrant on society.

He has gotten an award for being in detention more often than being in school.
He use to enjoy beating on other kids in the playground but now finds it easier to do it online plus he doesn't want to carry lunch money around any more, now he just has everybody use paypal.

Possibly the sloppiest emailer and texter on the face of the planet. He is constantly forgetting smiley faces and winks and is always texting messages to the wrong people.
He enjoys technology so much that nobody can stop him.

STOP

BLock

TELL

Because I can wait to see him in person
Because I respect myself
Because I want others to respect me
Because I don't know where it will end up
... What is your reason not to sext?

9 – 9:25am	Welcome and Introductions
9:25 – 9:50am	The Work in Limerick – Findings and Observations
9:50 – 10:15am	Barbara Coloroso—Bullying—a demonstration
10:15 – 11:05am	Panel: Law, Law Enforcement and Justice
11:05 – 11:30am	Carol Todd—A Perfect Storm
11:30 – noon	Panel: Cyberwellness
noon – 12:45pm	Panel: Youth Voices
12:45- 1:30pm	Lunch, Music, PIP and commentary
1:30 – 2:30pm	Panel: International Perspectives Italy, Spain, Canada, USA, Ireland, Wales, N. Ireland, England, the EU as a whole
2:30 – 3:45pm	Panel: Industry Best Practices and Role of Technology
3:45 – 4pm	Break, pics and commentary
4:00 – 4:15pm	Mustafa Ahmed
4:15 – 5:00pm	Panel: Inspiring Change
5:00 – 5:30pm	Wrap Up

Notes:

You Say Cyberbullying, I Say Being Rude!

When minors get into a fist fight, we often call it "bullying." But when adults get into a fist fight, we call it "assault and battery." Calling anything "bullying" somehow makes it less important, sadly. It denotes childhood activity, so we use it only when dealing with attacks between or among minors in cyberspace.

A rude communication or insult, especially when the student communicating the insult identifies himself or herself, is merely rude. It takes more than an insult to constitute cyberbullying.

The best way to determine whether something is merely rude or rises to the level of cyberbullying is to use a sliding scale, in which the frequency or scope of the communication and the nature of the message are taken into consideration. The more threatening the message or risky the activities for the target, the less frequent or public they must be to qualify as "cyberbullying." To complicate the issue, if the message is sent anonymously so that the student cannot evaluate the real risk of any threat, it becomes "cyberbullying," even if it was ultimately determined to be from a friend and, therefore, a joke and not a credible threat.

To simplify: "Cyberbullying" is a product of the nature of the message or activity designed to hurt another minor, the frequency and nature of the technology being used, and the credibility of the threat (which becomes higher if the target cannot determine the identity of the cyberbully).

Cyberbullying = nature of communications X frequency X identity/anonymity

Students understand this very well. Most don't consider a one-time rude or insulting communication to be cyberbullying. They think it needs to be repeated, or be a threat of bodily harm or a public posting designed to increase the hurt, embarrassment, or emotional damage to their target. And they are right.

Digital Anonymity:

1. **Think about anonymity. Is an anonymous attack worse than one where you know the attacker? Why?**
2. **Are there reasons that anonymous communications are helpful to youth?**
3. **Is there a way to combine the two, so communications can remain anonymous as long as cyberbullying does not occur. Then you own it or remove it. Identify yourself and stand behind your comment, or delete it.**

Report It, Don't Support It! Do You Report Cyberbullying When You Find It? Do you know what to report? Do you know how to make a report? Do you know that most reports are kept private and the person you report won't know you reported them.
Did you know that a big majority of the reports made are mis-reported (reported for the wrong reason, failing to provide important information, reporting things that don't constitute abuse.)

STOP Cyberbullying TOOLKIT

Why a Toolkit for schools? Because it starts and stops with schools. They are the first to know about bullying and cyberbullying (after the target in most cases). They are the only ones to fully appreciate the dynamics and the risks, and be able to frame solutions. They provide the only touchstone between home, the students, the community, and law enforcement. But, unless we can help schools understand what steps they need to take and help them with professional development and tools, it will just be one more thing we dump on already overloaded school administrators and educators. That's what this StopCyberbullying Toolkit was created to address.

With cyberbullying growing daily, a concerted effort by all of these stakeholders, managed through schools, is more important than ever before. The StopCyberbullying Toolkit contains practical tips, animations, activity sheets, games and printables, a risk management guide for schools, presentation materials for parents and students, first responder guides for community policing units and school resource officers, and fun activities for students of all ages. All are free for schools to use through the generous support of our sponsors and with the help of our strategic partners. It's everything Parry Aftab and WiredSafety have on cyberbullying and will be updated often with new tools, resources, and activities.

Our Mascot, Woody, checking out the latest MacBook Pro to prepare for the Summit.

What About the Law?

While we discuss some important laws and how they impact safety and risk management in the school, you will notice it is less about the wording or exact coverage of the laws themselves and far more about the legal approach. The laws will change, but most often the legal approaches don't. Instead of memorizing what exists today and worry about what will be adopted tomorrow, think in terms of 1. safety, 2. privacy, 3. security, and 4. authority. Most laws relate to one of these four important issues. If you learn to spot when they are impacted or implicated, you'll be fine.

When you seek to discover which laws might be applicable to punish the cyberbully, you need to think about the elements of the cyberbullying incident(s).

The Legal Elements

When you look at cyberbullying from the legal perspective, break it down to its elements:

- Is it threatening?
- Is it defamatory?
- Is it targeting teachers or school administrators? (Remember this isn't "cyberbullying" under our definition, but it is cyberharassment, given the adult's involvement.)
- Was it sent from school computers, during the school day, from a school-sanctioned event, or promoted in school?
- Was it from a home computer, off-school premises, and not involving a school sanctioned event?
- Has the person identified themselves?
- Was it sent while posing as someone else?
- Was it sent anonymously?
- Was it sent only to the target or was it publicized?
- What device was used?
- Who owns or legally controls that device? (Such as someone's cellphone being grabbed when they weren't looking.)
- Is it repeated? If so, how often?
- Did they break into the target's online account?
- Did they have legal access to the target's password (because it was given to them or stored on their computer)?

The range of legal options and potential legal liability include:

1. Criminal laws;
2. Constitutional and civil rights violations (depending on whether the state gives private rights of action);
3. School rules and regulations;
4. Regulatory agency regulations;
5. Hate laws;
6. Defamation;
7. Illegal intrusion laws;
8. Terrorism laws;
9. Hacking-related laws;
10. Extortion;
11. Sexual exploitation laws;
12. Dissemination, production, or possession of obscenity or child pornography;
13. Privacy laws;
14. Theft, vandalism, and criminal trespass;
15. Misappropriation; and
16. Harassment and bullying/cyberbullying-specific laws.

At-Risk Youth

The Harvard Berkman Center Internet Safety Technical Task Force (of which WiredSafety was one of the 29 members) found that students who were at risk in real life were at risk online. This shouldn't come as a surprise to school administrators or educators.

Angry and dysfunctional students will evidence their anger and dysfunction online as well as offline. The problems they have communicating in real life may be magnified online and they may be seen as a harasser when they do not intend it. They may have more vulnerability online, too. Other students who fear them in real life may feel much braver attacking them anonymously online.

Guidance counselors and social workers, as well as special education educators, should google their students to keep an eye on what they are posting online and what others may be posting about them online. Often, at-risk students don't use the same networks as their peers. Sites like VampireFreaks.com may be more attractive to these students and less obvious to other students in their school. Keep an eye out for new sites with special attraction to students at risk.

Sometimes students who are most at risk are also running afoul of the law. With police monitoring networks looking for crime plans, confessions, or boasting, keeping an eye out for these posts is important. Gangs are thriving online, recruiting new members, fundraising, and threatening other gangs and their members. The school gang team, if there is one, should be watching for online gang activities as well. Hate groups, neo-Nazis, white supremacists, and other bigotry and intolerance-themed groups should be monitored online to help prevent or forecast attacks before they hit.

Be very careful about mainstream students deciding to become vigilantes and creating cyberbullying campaigns to take on members of these at-risk groups.

My Pages:

My Pages:

Cyberbully-Proofing Your School (for Educators)

Risk management is a process. It's a combination of policies, procedures, and awareness. It's a package.

Start with taking an inventory. What technologies do you use at the school? What software and safety tools are being used? Are they being used effectively? Do you have a library media specialist? Technology program? Engaged network administrators? A school e-mail network or social network? Online learning tools? Do you filter or monitor school communications? Do you have an electronic use policy for employees? Do you use outside providers for technology? Do they offer tools, training, or educational resources? How much time, effort, and resources are you able/willing to devote to this?

Are you reacting to a current problem? Has cyberbullying been an issue in your school? Are you just interested in improving safety? Do you have a grant or funding opportunity that requires you to address cyberbullying? Are there new or existing laws that require that you take action?

Are your students connected outside of school? If so, how? Home broadband access? Dial-ups? Community and library access only? Cellphones? Handheld or gaming devices? Is it a single gender school? Do you have special-needs students in separate programs or mainstreamed? Do you have an ethics or offline bullying program within the school already? Is there tension you are seeking to defuse? Are the students engaged or unmotivated on this issue?

What about parents? How tech-literate are they? How connected are they to both the school and technology? What's the most effective way of reaching them—online, offline, newsletters, e-mail, mom groups, Facebook?

Do you have an effective school resource officer or community policing officer? Are they engaged in cybersafety issues? Are they willing to work in developing risk management programs with the school? Do they have the trust and respect of the parents?

Once you understand the lay of the land, set goals. They can be long and short range plans, but once you set them, you can start building a program to help meet those goals. Set out the plan in writing. Get all stakeholders involved. Be flexible in defining and revising the plan. Finally, get all stakeholders committed to helping reach the goals.

You may be able to tackle this without additional funding. This StopCyberbullying Toolkit contains hundreds of thousands of dollars worth of resources and materials, free for schools. Student creativity and commitment is powerful and also free. Tap parents' skills and resources. Reach out to the local business community and your Internet service providers. Ask your cellphone providers to get involved. Gather together the best you can and start with something tangible. Host a StopCyberbullying Day at the school. Get all students to take the StopCyberbullying Pledge and create posters promoting the StopCyberbullying events. Have parents attend an evening event to learn about cyberbullying and encourage students to share their stories. Create a suggestion box for students and find ways to engage the whole staff.

Reach out to local media. Offer them insight and expertise in covering cyberbullying news in exchange for promoting your programs and creating awareness.

Start small, but end big. Build on the strength of others. Use the StopCyberbullying materials and create new ones of your own. Then recycle them by sharing them with us so we can get them out to others who need them. If you use something, improve it before you give it back. Parry's mom used to return the borrowed cup of sugar with a pound cake. Share pointers and research. Conduct research using surveys created or approved by WiredSafety and share the results so we can publicize them.

Talk the talk, walk the walk. Build an atmosphere of kindness, respect, and caring.

CyberWellness.com - Professional Development and Resources

A new program to educate and empower medical professionals

wired SAFETY

The Mission:

- To provide trustworthy, relevant resources, tools, training and education to medical professionals to share with their patients and their family
- To create a corps of educated, trusted professionals to deliver credible cyberwellness information and resources to their constituent groups
- To enable and empower intervention specialists to address identified risks “just in time” through existing relationships
- To help customize regional, respectful and relevant resources, materials and approaches for multi-ethnic/lingual/cultural communities

Redefining Our Relationship with Digital Technology

wired SAFETY

Cyberwellness.com

A New Network, Resource and Guide to Help Everyone Find Better Balance in the Digital World

Pre-Subscription Sponsors:

Harrah’s®