What is cyberbullying, exactly?

"Cyberbullying" is when a child, preteen or teen is tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another child, preteen or teen using the Internet, interactive and digital technologies or mobile phones. It has to have a minor on both sides, or at least have been instigated by a minor against another minor. Once adults become involved, it is plain and simple cyber-harassment or cyberstalking. Adult cyber-harassment or cyberstalking is NEVER called cyberbullying.

It isn't when adult are trying to lure children into offline meetings, that is called sexual exploitation or luring by a sexual predator. But sometimes when a minor starts a cyberbullying campaign it involves sexual predators who are intrigued by the sexual harassment or even ads posted by the cyberbullying offering up the victim for sex.

The methods used are limited only by the child's imagination and access to technology. And the cyberbully one moment may become the victim the next. The kids often change roles, going from victim to bully and back again.

Children have killed each other and committed suicide after having been involved in a cyberbullying incident.

Cyberbullying is usually not a one time communication, unless it involves a death threat or a credible threat of serious bodily harm. Kids usually know it when they see it, while parents may be more worried about the lewd language used by the kids than the hurtful effect of rude and embarrassing posts.

Cyberbullying may arise to the level of a misdemeanor cyberharassment charge, or if the child is young enough may result in the charge of juvenile delinquency. Most of the time the

cyberbullying does not go that far, although parents often try and pursue criminal charges. It typically can result in a child losing their ISP or IM accounts as a terms of service violation. And in some cases, if hacking or password and identity theft is involved, can be a serious criminal matter under state and federal law.

When schools try and get involved by disciplining the student for cyberbullying actions that took place off-campus and outside of school hours, they are often sued for exceeding their authority and violating the student's free speech right. They also, often lose. Schools can be very effective brokers in working with the parents to stop and remedy cyberbullying situations. They can also educate the students on cyberethics and the law. If schools are creative, they can sometimes avoid the claim that their actions exceeded their legal authority for off-campus cyberbullying actions. We recommend that a provision is added to the school's acceptable use policy reserving the right to discipline the student for actions taken off-campus if they are intended to have an effect on a student or they adversely affect the safety and well-being of student while in school. This makes it a contractual, not a constitutional, issue.

How cyberbullying works

There are two kinds of cyberbullying, direct attacks (messages sent to your kids directly) and cyberbullying by proxy (using others to help cyberbully the victim, either with or without the accomplice's knowledge). Because cyberbullying by proxy often gets adults involved in the harassment, it is much more dangerous

Cyberbullying by proxy

Cyberbullying by proxy is when a cyberbully gets someone else to do their dirty work. Most of the time they are unwitting accomplices and don't know that they are being used by the cyberbully. Cyberbullying by proxy is the most dangerous kind of cyberbullying because it often gets adults involve in the harassment and people who don't know they are dealing with a kid or someone they know.

"Warning" or "Notify Wars" are an example of cyberbullying by proxy. Kids click on the warning or notify buttons on their IM screen or e-mail or chat screens, and alert the ISP or service provider that the victim has done something that violates their rules.If the victim receives enough warnings or notifications, they can lose their account. The service providers are aware of this abuse, and often check and see if the warning were justified. But all the cyberbully has to do is make the victim angry enough to say something rude or hateful back. Then, BINGO! they warn

them, making it look like the victim had started it. In this case, the ISP or service provider is the innocent accomplice of the cyberbully.

Sometimes the victim's own parents are too. If the cyberbully can make it look like the victim is doing something wrong, and the parents are notified, the parents will punish the victim. Alyssa, one of our Teenangels, had this happen to her. To learn more about her cyberbullying problem, read Alyssa's story.

Cyberbullying by proxy sometimes starts with the cyberbully posing as the victim. They may have hacked into their account or stolen their password. They may have set up a new account pretending to be the victim. But however they do it, they are pretending to be the victim and trying to create problems for the victim with the help of others.

The most typical way a cyberbullying by proxy attack occurs is when the cyberbully gets control of the victim's account and sends out hateful or rude messages to everyone on their buddy list pretending to be the victim. They may also change the victim's password so they can't get into their own account. The victim's friends get angry with the victim, thinking they had sent the messages without knowing they have been used by the cyberbully. But it's not always this minor. Sometimes the cyberbully tries to get more people involved.

For example...Mary wants to get Jennifer back for not inviting her to her party. She goes online and, posing as Jennifer, posts "I hate Brittany, she is so stupid, ugly and fat!" on buddyprofile.com. Mary may tell Brittany and her friends that she read the post on buddyprofile.com and blames Jennifer for being mean. Brittany and her friends now start attacking Jennifer, and may report her to buddyprofile.com or her school. They are doing Mary's dirty work for her. Mary looks like the "good guy" and Jennifer may be punished by her parents, lose her account with buddyprofile.com and get into trouble at school. And Brittany and her friends may start to cyberbully Jennifer too.

Sometimes it is much more serious than that. When cyberbullies want to get others to do their dirty work quickly, they often post information about, or pose as, their victim in hate group chat rooms and on their discussion boards. Cyberbullies have even posted this information in child molester chat rooms and discussion boards, advertising their victim for sex. They then sit back and wait for the members of that hate group or child molester group to attack or contact the victim online and, sometimes, offline.

For this to work, the cyberbully needs to post offline or online contact information about the victim. Real information, not the account they used to impersonate the victim (if they are posing

as the victim to provoke an attack). For example...Jack is angry that Blake was chose as captain of the junior varsity basketball team. Blake is black. Jack finds a white supremist group online and posts in their chat room that Blake said nasty things about whites and their group in particular. He then posts Blake's cell phone number and screen name. People from the group start calling and IMing Blake with threats and hateful messages. Jack has no idea how much danger he has placed Blake in, and Blake doesn't know why he in under attack. In cases of cyberbullying by proxy, when hate or child molester groups are involved, they victim is in danger of physical harm and law enforcement must be contacted immediately.

Can you think of examples of cyberbullying by proxy? Share them with us and other kids, preteens and teens here at the site. We'll never use your name or personally identifying information, share it with others or bother you. Read our privacy policy to know how we use your information. You should always read a privacy policy before submitting anything to anywhere online.

Why do kids cyberbully each other?

Who knows why kids do anything? When it comes to cyberbullying, they are often motivated by anger, revenge or frustration. Sometimes they do it for entertainment or because 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. Some do it by accident, and either send a message to the wrong recipient or didn't think before they did something. The Power-hungry do it to torment others and for their ego. Revenge of the Nerd may start out defending themselves from traditional bullying only to find that they enjoy being the tough guy or gal. Mean girls do it to help bolster or remind people of their own social standing. And some think they are righting wrong and standing up for others.

Because their motives differ, the solutions and responses to each type of cyberbullying incident has to differ too. Unfortunately, there is no "one size fits all" when cyberbullying is concerned. Only two of the types of cyberbullies have something in common with the traditional schoolyard bully. Experts who understand schoolyard bullying often misunderstand cyberbullying, thinking it is just another method of bullying. But the motives and the nature of cybercommunications, as well as the demographic and profile of a cyberbully differ from their offline counterpart.

Take a stand against cyberbullying

Education can help considerably in preventing and dealing with the consequences of cyberbullying. The first place to begin an education campaign is with the kids and teens

themselves. We need to address ways they can become inadvertent cyberbullies, how to be accountable for their actions and not to stand by and allow bullying (in any form) to be acceptable. We need to teach them not to ignore the pain of others.

Teaching kids to "Take 5!" before responding to something they encounter online is a good place to start. Jokingly, we tell them to "Drop the Mouse! And step away from the computer and no one will get hurt!" We then encourage them to find ways to help them calm down. This may include doing yoga, or deep-breathing. It may include running, playing catch or shooting hoops. It may involve taking a bath, hugging a stuffed animal or talking on the phone with friends. Each child can find their own way of finding their center again. And if they do, they will often not become a cyberbully, even an inadvertent cyberbully. Teaching them the consequences of their actions, and that the real "Men in Black" may show up at their front door sometimes helps. Since many cyberbullying campaigns include some form of hacking or password or identity theft, serious laws are implicated. Law enforcement, including the FBI, might get involved in these cases.

But we need to recognize that few cyberbullying campaigns can succeed without the complacency and the often help of other kids. If we can help kids understand how much bullying hurts, how in many cases (unlike the children's chant) words *can* hurt you, fewer may cooperate with the cyberbullies. They will think twice before forwarding a hurtful e-mail, or visiting a cyberbullying "vote for the fat girl" site, or allowing others to take videos or cell phone pictures of personal moments or compromising poses of others. Martin Luther King, Jr. once said that in the end we will remember not the words of our enemies, but the silence of our friends. We need to teach our children not to stand silently by while others are being tormented. While it is crucial that we teach them not to take matters into their own hands (and perhaps become a "vengeful angel" cyberbully themselves) they need to come to us. And if we expect them to trust us, we need to be worthy of that trust. (Read more about this at "**Goldilocks and the cyberbullies...not too hot and not too cold**," a guide for parents.)

And, in addition to not lending their efforts to continue the cyberbullying, if given an anonymous method of reporting cyberbullying Web sites, profiles and campaigns, kids can help put an end to cyberbullying entirely. School administration, community groups and even school policing staff can receive these anonymous tips and take action quickly when necessary to shut down the site, profile or stop the cyberbullying itself.

They can even let others know that they won't allow cyberbullying, supporting the victim, making it clear that they won't be used to torment others and that they care about the feelings

of others is key. Martin Luther King, Jr. once said "In the end, we will remember not the words of our enemies, but the silence of our friends."

We need to teach our children that silence, when others are being hurt, is not acceptable. If they don't allow the cyberbullies to use them to embarrass or torment others, cyberbullying will quickly stop. It's a tall task, but a noble goal. And in the end, our children will be safer online and offline. We will have helped create a generation

Preventing cyberbullying

Educating the kids about the consequences (losing their ISP or IM accounts) helps. Teaching them to respect others and to take a stand against bullying of all kinds helps too.

How can you stop it once it starts?

Because their motives differ, the solutions and responses to each type of cyberbullying incident has to differ too. Unfortunately, there is no "one size fits all" when cyberbullying is concerned. Only two of the types of cyberbullies have something in common with the traditional schoolyard bully. Experts who understand schoolyard bullying often misunderstand cyberbullying, thinking it is just another method of bullying. But the motives and the nature of cybercommunications, as well as the demographic and profile of a cyberbully differ from their offline counterpart.

What is the school's role in this?

When schools try and get involved by disciplining the student for cyberbullying actions that took place off-campus and outside of school hours, they are often sued for exceeding their authority and violating the student's free speech right.

[**Learn more...**]

What's the parents' role in this?

Parents need to be the one trusted place kids can go when things go wrong online and offline. Yet they often are the one place kids avoid when things go wrong online.

[**Learn more...**]

Take a stand against cyberbullying

Education can help considerably in preventing and dealing with the consequences of cyberbullying. The first place to begin an education campaign is with the kids and teens themselves. We need to address ways they can become inadvertent cyberbullies, how to be

accountable for their actions and not to stand by and allow bullying (in any form) to be acceptable. We need to teach them not to ignore the pain of others.

Teaching kids to "Take 5!" before responding to something they encounter online is a good place to start. Jokingly, we tell them to "Drop the Mouse! And step away from the computer and no one will get hurt!" We then encourage them to find ways to help them calm down. This may include doing yoga, or deep-breathing. It may include running, playing catch or shooting hoops. It may involve taking a bath, hugging a stuffed animal or talking on the phone with friends. Each child can find their own way of finding their center again. And if they do, they will often not become a cyberbully, even an inadvertent cyberbully. Teaching them the consequences of their actions, and that the real "Men in Black" may show up at their front door sometimes helps. Since many cyberbullying campaigns include some form of hacking or password or identity theft, serious laws are implicated. Law enforcement, including the FBI, might get involved in these cases.

But we need to recognize that few cyberbullying campaigns can succeed without the complacency and the often help of other kids. If we can help kids understand how much bullying hurts, how in many cases (unlike the children's chant) words *can* hurt you, fewer may cooperate with the cyberbullies. They will think twice before forwarding a hurtful e-mail, or visiting a cyberbullying "vote for the fat girl" site, or allowing others to take videos or cell phone pictures of personal moments or compromising poses of others. Martin Luther King, Jr. once said that in the end we will remember not the words of our enemies, but the silence of our friends. We need to teach our children not to stand silently by while others are being tormented. While it is crucial that we teach them not to take matters into their own hands (and perhaps become a "vengeful angel" cyberbully themselves) they need to come to us. And if we expect them to trust us, we need to be worthy of that trust. (Read more about this at "**Goldilocks and the cyberbullies...not too hot and not too cold**," a guide for parents.)

And, in addition to not lending their efforts to continue the cyberbullying, if given an anonymous method of reporting cyberbullying Web sites, profiles and campaigns, kids can help put an end to cyberbullying entirely. School administration, community groups and even school policing staff can receive these anonymous tips and take action quickly when necessary to shut down the site, profile or stop the cyberbullying itself.

They can even let others know that they won't allow cyberbullying, supporting the victim, making it clear that they won't be used to torment others and that they care about the feelings of others is key. Martin Luther King, Jr. once said "In the end, we will remember not the words of our enemies, but the silence of our friends."

We need to teach our children that silence, when others are being hurt, is not acceptable. If they don't allow the cyberbullies to use them to embarrass or torment others, cyberbullying will quickly stop. It's a tall task, but a noble goal. And in the end, our children will be safer online and offline. We will have helped create a generation of good cybercitizens, controlling the technology instead of being controlled by it.

Stop, block and tell

If you are targeted by a cyberbully:

- **STOP!**
  Don't do anything. Take 5! to calm down.
- **Block!**
  Block the cyberbully or limit all communications to those on your buddy list.
- **and Tell!**
  Tell a trusted adult, you don't have to face this alone.
  Report cyberbullying to wiredsafety.org

Cyberbullying Hurts!

Telling the difference between flaming, cyber-bullying and harassment and cyberstalking (A guide for law enforcement)

It's not always easy to tell these apart, except for serious cases of cyberstalking, when you "know it when you see it." And the only difference between "cyberbullying" and cyber-harassment is the age of both the victim and the perpetrator. They both have to be under-age.

When you get a call, your first response people need to be able to tell when you need to get involved, and quickly, and when it may not be a matter for law enforcement. It might help to start by running through this checklist. If the communication is only a flame, you may not be able to do much about it. (Sometimes ISPs will consider this a terms of service violation.) But the closer it comes to real life threats the more likely you have to get involved as law enforcement. We recommend that law enforcement agents ask parents the following questions. Their answers will help guide you when to get involved and when to recommend another course of action.

The kind of threat:

- The communication uses lewd language
- The communication insults your child directly ("You are stupid!")
- The communication threatens your child vaguely ("I'm going to get you!")
- The communication threatens your child with bodily harm. ("I'm going to beat you up!")
- There is a general serious threat. ("There is a bomb in the school!" or "Don't take the school bus today!")
- The communication threatens your child with serious bodily harm or death ("I am going to break your legs!" or "I am going to kill you!")

The frequency of the threats:

- It is a one-time communication
- The communication is repeated in the same or different ways
- The communications are increasing
- Third-parties are joining in and communications are now being received from (what
- appears to be) additional people

The source of the threats:

- Your child knows who is doing this
- Your child thinks they know who is doing this
- Your child has no idea who is doing this
- The messages appear to be from several different people

The nature of the threats:

- Repeated e-mails or IMs
- Following the child around online, into chat rooms, favorite Web sites, etc.
- Building fake profiles, Web sites or posing as your child's e-mail or IM
- Planting statements to provoke third-party stalking and harassment
- Signing your child up for porn sites and e-mailing lists and junk e-mail and IM.
- Breaking in to their accounts online
- Stealing or otherwise accessing their passwords
- Posting images of the child online (taken from any source, including video and photo phones)
- Posting real or doctored sexual images of the child online

- Sharing personal information about the child
- Sharing intimate information about the child (sexual, special problems, etc.)
- Sharing contact information about the child coupled with a sexual solicitation ("for a good time call …" or "I am interested in [fill in the blank] sex…")
- Reporting the child for real or provoked terms of service violations ("notify wars" or "warning wars")
- Encouraging that others share their top ten "hit lists," or ugly lists, or slut lists online and including your child on that list.
- Posting and encouraging others to post nasty comments on your child's blog.
- Hacking your child's computer and sending your child malicious codes.
- Sending threats to others (like the president of the United States) or attacking others while posing as your child.
- Copying others on your child's private e-mail and IM communications.
- Posting bad reviews or feedback on your child without cause.
- Registering your child's name and setting up a bash Web site or profile.
- Posting rude or provocative comments while posing as your child (such as insulting racial minorities at a Web site devoted to that racial minority).
- Sending spam or malware to others while posing as your child.
- Breaking the rules of a Web site or service while posing as your child.
- Setting up a vote for site (like "hot or not?") designed to embarrass or humiliate your child.
- Masquerading as your child for any purpose.
- Posting your child's text-messaging address or cell phone number online to encourage abuse and increase your child's text-messaging or cell phone charges.
- Launching a denial of service attack on your child's Web site
- Sending "jokes" about your child to others or mailing lists.

The more repeated the communications are, the greater the threats (or enlarging this to include third-parties) and the more dangerous the methods, the more likely law enforcement or legal process needs to be used. If personal contact information is being shared online, this must be treated very seriously.

If the child thinks they know who is doing this, that may either make this more serious, or less. But once third-parties are involved (hate groups, sexually-deviant groups, etc.) it makes no difference if the person who started this is a young seven year old doing it for a laugh. It escalates quickly and can be dangerous.

It's best to work out relationships with the big ISPs in your area well before you need them. Find their offline contact information, including off hours. Learn how to track an IP address and preserve evidence. And make sure that you issue your subpoenas in the form they need, using your time zone for tracking the dynamic IP addresses of record. Many ISPs discard the subscriber/IP data after a week to thirty day period. So time is crucial. If you need to get your paperwork together, send them a quick note asking them to preserve the records pending your formal subpoena. They will usually do this on a less formal request on law enforcement letterhead.

Are you a cyberbully?

Often, people who are victims are also bullies. Before you feel too bad for yourself, take the quiz below to find if you, too, are part of the cyberbullying problem! Rate yourself on the following point scale according to if, and how many times, you have done the below activities. Give yourself 0 points if you've never done it, 1 point if you have done it 1 or 2 times, 2 points if you have done it 3-5 times, 3 points if you have done it more than 5 times.

Have you ever...

___Signed on with someone else's screen name to gather info?

___Sent an e-mail or online greeting card from someone's account?

___Impersonated someone over IM or online?

___Teased or frightened someone over IM?

___Not told someone who you really are online, telling them to "guess"?

___Forwarded a private IM conversation or e-mail without the permission of the other person?

___Changed your profile or away message designed to embarrass or frighten someone?

___Posted pictures or information about someone on a Web site without their consent?

___Created an Internet poll, either over IM or on a Web site, about someone without their consent?

___Used information found online to follow, tease, embarrass or harass someone in person?

___Sent rude or scary things to someone, even if you were just joking?

___Used bad language online?

___Signed someone else up for something online without their permission?

___Used an IM or e-mail address that looked like someone else's?

___Used someone else's password for any reason without their permission?

___Hacked into someone else's computer or sent a virus or Trojan horse to them?

___Insulted someone in an interactive game room?

___Posted rude things or lies about someone online?

___Voted at an online bashing poll or posted to a guestbook saying rude or mean things?

Now calculate your total score:

0 – 5 Points: Cyber Saint

Congratulations! You're a cyber saint! Your online behavior is exemplary! Keep up the good work!

6-10 Points: Cyber Risky

Well, you're not perfect, but few people are. Chances are you haven't done anything terrible and were just having fun, but try not to repeat your behaviors, since they are all offenses. Keep in mind the pain that your fun might be causing others!

11-18 Points: Cyber Sinner

Your online behavior needs to be improved! You have done way too many cyber no-no's! Keep in mind that these practices are dangerous, wrong, and punishable and try to be clean up that cyber record!

More than 18: Cyber Bully

Put on the brakes and turn that PC/MAC/text-messaging device around! You are headed in a very bad direction. You qualify, without doubt, as a cyberbully. You need to sign off and think about where that little mouse of yours has been clicking before serious trouble results for you and/or your victim(s), if it hasn't happened already!

Take 5!

Put down the mouse and step away from the computer…and no one will get hurt!

The Internet and mobile technology are very powerful. But if misused, they can also be dangerous to yourself and others. Most of the time we make sure that people are old enough and pass special tests before they drive cars, operate heavy machinery or otherwise use potentially powerful technology. This is for their safety and the safety of others.

But the Internet is different. It's kids who show the adults how to use it. And kids who learn quickly how to abuse it as well. Unfortunately, the abuses are limited only by their limitless imaginations and tech skills.

Our kids use the Internet the way we used the phone when we were young. They "talk" using text-messaging and instant messaging, often at the same time they are chatting on the phone with the same people. It may be hard for parents to conceive of the ways our kids use technologies as part of their everyday lives.

I was talking to some middle school students recently, and asked them how they would feel if they didn't have the Internet anymore. They told me that the Internet is their "life!" It's how the learn, how they communicate, how they socialize and how they share information.

But the casual nature of the way they use the technology leads to abuse and mistakes. The typed word doesn't clarify tone. It doesn't, without more (like an emoticon :oP or an acronym like "jk" which is the short form for "just kidding"), convey the kind of information we obtain when we hear the person's voice or watch their body-language or eye-contact. We make judgments based on how the words appear to us. And those judgments are often wrong. They are often taken out of context and misunderstood.

That results in hurt feelings, anger, frustration and feeling threatened. And when people, especially kids, act out of anger, frustration or fear things get out-of-hand quickly. Like drinking and driving, emotions and the Internet should never be mixed. Emotions create a situation where we click before thinking. We don't think about how the person on the other end may misunderstand our message or our intentions. We don't think at all.

The best way to counter this problem is by teaching our children (and ourselves) to Take 5! - put down the mouse and step away from the computer. By not reacting and taking the time to calm down, we can avoid becoming a cyberbullying ourselves. What can we do for 5 minutes to help us calm down? Kids have suggested: throwing a baseball or shooting hoops, baking cookies, reading, napping, taking a walk or a run, watching TV, talking to a friend and hugging a stuffed animal.

A Checklist for Cybercommunications:

Before sending that e-mail or posting on that Web site or bulletin board, think before you click "send." Re-read what you were going to send. If it meets any of these factors, don't send it until you fix them. And if you can't fix them, maybe you shouldn't send it at all.

It's so easy for anyone to misunderstand e-mails and cybercommunications. We have to be very very careful to make them clear and help others to understand what we really mean. We also need to be careful not to hurt others and be good netizens.

- **Start by making sure you are sending things to the right place, that it arrives and that the right person gets it.**

Is it addressed to the right person? Are you sure? Have you checked the spelling and the screen name carefully? Are they in your address book or on your buddy list already? The easiest way to make sure that you have their correct screen name or e-mail address is to save it automatically when they send you something. Parents should input their children's approved correspondents into their buddy lists and address books to make sure that it is done correctly. Also, people (especially kids) change their e-mail addresses and screen names often. Make sure you are using the most up-to-date one.

Also, don't be so sure that your e-mail makes it to the person you sent it to. With so many junk e-mails and viruses being sent these days, most Internet service providers are using spam-blocking technology to block and filter messages they think may be spam. Many innocent messages are caught in the spam-filters and never get delivered anymore. Some people are also using their own anti-spam software that may block your e-mail. Remind your friends to add your

e-mail address and screen name to their approved list so that you won't be blocked by accident and warn them in advance before using a new address or screen name. Depending on which e-mail service you use, you may be able to track your message and see if it is ever delivered, and sometimes if it is even read. There are other applications you can use as well. It's good netiquette to ask the person before sending something to track whether they have opened or read the e-mail before using it. But just because you send something, don't get angry if the other person doesn't reply. First make sure they received it. (And make sure that they aren't blocked by your e-mail filters or spam-blockers either.)

Sometimes one family will use the same e-mail address or screen name for everyone. It could be embarrassing if you send a personal and private message to someone and their parents or older brother reads it instead. Check first. Also, many parents read their kids e-mails. Check with your friends and see if their e-mails are reviewed by their parents. You may want to be more careful if they do.

- **Is it worth sending? Don't waste peoples' time or bandwidth with junk, chain e-mails and false rumors**

Some of your friends and people you know love getting lots of e-mail, IMs and jokes. Others don't. Before you start sending lots of jokes and attachments to someone, find out if it's okay first. And if they tell you they are busy, respect their time. It never hurts to ask first. That way people will look forward to getting your e-mails and cybercommunications instead of ignoring them. Also, don't send long e-mails to people who only read short ones, or short ones to people who like long ones without explaining why.

Don't send chain e-mails. They clog up e-mail servers, especially at school. And sometimes scare people, especially younger kids. Also, sometimes bad people who are looking to find kids online use them to spy on e-mails and find new kids to contact. (You can read more about chain e-mails at "e-mail netiquette and safety.")

Also, never send anything you haven't confirmed as being true. Many hoaxes and cyber-rumors are sent by people who just blindly forwarded them on, without checking to see if they are true. (You can read more about urban legends, hoaxes and cyber-rumors and how to check and see if they are true or not at our "Truth or Hype" section.)

If you are going to send an e-mail to someone famous you found online, think about what you're going to say. Many of these people answer select e-mails, and you want yours to be answered, not ignored. Also, if you ask them for something that is inappropriate (like helping you write your

term paper) or something you should have found on your own (like their biography or information readily found at their Web site) they probably won't bother answering you.

Also, don't just send a "hi!" message without more. The worse that will happen is that it will be caught in the spam-filter or ignored. The best that will happen is that they will say "hi" back. What good is that? Also, never send an attachment to someone you don't know. They will probably automatically delete it. You can almost always include a photo or the document in the e-mail itself, instead of having to attach it. And make sure that you have allowed them to reply, without finding that they are blocked by parental controls or your e-mail filters.

- **Proofread and spell-check your e-mails and make sure they know who you are**

Many messages are never understood or are misunderstood because people left out words, or said things unclearly, or misspelled words. While your e-mails don't have to be formal works of art, your should make them clear. If they are important enough to send, they are important enough to be understood. The rules for instant messaging are different and more grammar mistakes and spelling errors are accepted there.

Also make sure that you re-read what you are sending to make sure it says what you want it to say. If something could be misunderstood, or understood two different ways, either re-write it or use an emoticon to let them know which meaning you used. Don't use shorthand or acronyms they don't understand. And if you are referring to someone else, make sure they know who you are talking about.

Also make sure that you sign your e-mails and cybercommunications with a name the recipient will recognize, if you aren't using your normal screen name. Don't' give away personal information, but telling them that this is a new account or screen name and your old one was [fill in the blank] helps your message get read, instead of trashed. Putting that in the subject line may help.

- **Don't attack others online, say anything that could be considered insulting or that is controversial**

Until you get to know someone very well, it's always best to stay away from controversial topics, like politics, religion, race, sex, nationalism, war, special physical or mental limitations, money and gender-based issues. Once you get to know each other well-enough to know what is acceptable, you can get into these topics online, but even then, be very careful. Most cyber-problems start when people are talking about these and similar topics.

And be especially careful when dealing with people form other cultures and countries online. What may be perfectly acceptable in the United States may not be acceptable in Japan, or England, or Hong Kong, or New Zealand. Watch what they say and how they say it before jumping in. Be extra polite and respectful and don't be afraid to ask how they do things where they live. It's a great way to learn.

If someone tells you that you hurt their feelings, find out how and apologize. Let them know when you did things without meaning to. If they lash out at you, thinking you did it on purpose, before you attack them back, try explaining that it was accidental.

Don't use all capital letters (considered shouting online) and be careful about using bad language or being provocative. Don't intentionally say anything to hurt some else's feelings or invade their privacy online or offline. And always scan your system for viruses and malicious code so that you don't send a virus by accident to someone else. (Use a good anti-virus program on anything you receive or download to make sure you don't pick up any viruses.)

- **Don't forward other people's e-mails without their permission or share their personal information**

Sometimes, without realizing it, we copy someone new on an e-mail thread. It might contain personal information or a personal communication that someone else shared with only you three levels down and you didn't realize that you were now allowing others to read it. Either delete all but the most recent message when forwarding it, or re-read the older threaded messages before forwarding to make sure nothing personal is in those messages. Many private things slip through that way by mistake.

- **Are you angry when you are writing this message?**

If you are writing the e-mail, instant message or post when you are angry, review it carefully. Also take the time to cool down before sending it and check the tips for avoiding cyberfights, by using the tips we learn in Take 5!

Are you replying to something that is designed to insult you, flame you, cyber-bully you or harass you? If so, think again. These things go away much faster if you don't reply at all. The person sending them is looking for a reaction. They soon get tired and go away if they don't get any. Also, you should let your parents or teachers know if you are receiving hateful or threatening cybercommunications or if you receive something that hurts your feelings or makes you feel bad. You are entitled not to be attacked online and enjoy e-mail and cybercommunications without worrying about nasty people.

- **Don’t reply to spam, even to ask to be removed from their mailing list**

Spammers buy lists of millions of e-mail addresses and instant messaging screen names. Harvesting programs gather up these addresses wherever they can find them online, in chat rooms, on message boards, from chain e-mails and registrations. So, many of these addresses are old and don’t work. If you reply, one of two things happens. You either have sent a reply to a fake address they have used to send the e-mails from, or you have now let them know that your address is a good one and you will receive many more messages. They will even sell your address for more money, since they can now promise that you have read the spam messages you receive.

While your e-mail service provider may ask you to forward spam to their TOS (terms of service violations address), you shouldn’t bother. Instead, use a good anti-spam program or the dual e-mail trick. [link to dual e-mail trick])

- **How private is the message you are sending? Are you willing to have others read this message or forward it to others without your permission?**

E-mails get misdelivered all the time. And sometimes the people we send them to share our communications with others without asking us first. (This includes logs of our chat room discussions and of instant messaging.) The courts allow others to read your e-mails under special circumstances. Don’t ever say anything in a cybercommunication you wouldn’t be willing to allow someone else to read. We always tell people not to say anything they wouldn’t write on a postcard they send through the mail. Sometimes when our friends get angry with us, they intentionally post our e-mails on public Web sites or send them to others. If you are going to share something very private, it’s best to use the phone or person-to-person communications (obviously only with people you know in real life).

When students apply for jobs or internships the recruiter will sometimes “Google them” first. We have seen many cases where old messages they posted when they were much younger and didn’t realize would turn up in an online search cost someone an internship position or a job. (It’s always a good idea to “Google yourself” regularly and make sure nothing turns up that you would be embarrassed about or that gives away personal information about you online.)

Also, many parents and schools monitor communications. This means they can read what you have written. Have you written anything they can’t read? And if you are using a family account that one of your parents uses for work e-mail, their boss may be monitoring e-mails too. That could be very embarrassing for everyone and may cost your parent their job.

Instant messaging 101

Instant messaging is what kids do online more than anything else. There are many different kinds of instant messaging technology, and most are free. AIM (AOL's instant messenger free application) is the most popular, but MSN's free instant messenger application and Yahoo's free instant messenger application are also very popular.

IM is more like talking than e-mail is. You can do it while playing games, or doing homework or even while talking on the telephone to the same people you are IMing. Some kids IM certain kinds of things while talking about others in the same conversation. IMs are used to emphasize certain points, or to add additional thoughts or information.

Text-messaging devices, like mobile phones and mobile text-messengers, are very popular with kids as well. They are used to chat, send messages and communicate with their friends and, increasingly, parents. Many schools have banned these devices, as kids have learned to use them to cheat on tests (IMing each other for the answers) or to pass messages in class.

Some of the newer applications allow voice IM, and photo or video IMs too.

Attachments, including malicious code and viruses, can be sent by IM too. And spam has moved over the IM, being renamed SPIM to differentiate it from its e-mail counterpart.

Most IM safety tips mirror e-mail and chat safety tips. Not sharing personal information with strangers, making sure you really know the person you are IMing, checking all attachments with an updated anti-virus program are all at the top of the lists. Knowing how to use the privacy and security settings for your IM application is essential, as well. Blocking any person who bothers you, or who sends you unwanted or inappropriate messages or attachments is very important. And blocking anyone not on your approved or buddy list is too.

Cyberbullying, cyberstalking and harassment often occur using IM applications. Trojan horse hacking and virus programs are often sent that way too. Since many screens are open at once, kids are not as careful when opening IMs as they are with e-mails.

When things go wrong, it's harder to trace an IM than an e-mail. They don't use the traditional headers used by e-mail applications, so spotting the IM source isn't easy. And finding who is behind the IM message is much harder with IM as well. Many e-mail accounts require a paid subscription and can be traced to the sender easily. IM accounts, like many free web-based e-

mail accounts, can be opened by anyone and shut down as fast. No proof of who you really are is required. And, while chat rooms often receive the biggest blame for online sexual predators, in the U.S. at least most cases involve IM, not chat. That's why using a logging or monitoring product that will capture IMs is important in case anything goes wrong. Otherwise, the message is lost in the ether and taking any disciplinary actions or legal action is difficult, if not impossible.

Many kids use more than one IM application, since with the exception of Trillian, they only communicate with others using the same IM platform. And having eight or nine IM communications open at the same time isn't unusual at all, when kids are IMing. Because it is more like talking than writing, kids find themselves breaking the privacy and safety rules when using IM more than in other applications, except chat. And IMing with strangers is much more dangerous than chatting with strangers. I always explain that most of us would prefer that our children are approached on a full playground, rather than one-on-one, if they encounter a sexual predator. There is strength and safety in groups. When approached one-to-one our children are often easier prey.

But banning IM is not an option. The kids would feel and be isolated if their friends communicate using IM. They wouldn't know what social events are planned and wouldn't be informed when everyone else learns about things. It's much better to screen out strangers and teach ourselves and others not to respond when a stranger sends an IM with "hi!" and tries to make us "guess" who they are. If they are really someone you know, they will find a way to let you know. Block and report any misuse as well.

The only way to monitor IMs and to capture them for any future reporting or prosecution needs is to use a monitoring software, like Spectorsoft.

Sticks and Stones - Defaming Others Online

Sticks and stones will break their bones, but words will never hurt them—right? Wrong! While the First Amendment gives us the right of free speech, it does not give us the right to say false and horrible things about others. In the United States, someone whose reputation is damaged by a false statement made by another can sue that person for defamation. (Libel is when the defamatory statement is written, and slander is when it is spoken.) Under rare circumstances, such statements and the way they are delivered may rise to the level of cyberstalking or harassment, considered a crime in more than 46 states.

Unfortunately, since the advent of the Web, many are taking their grievances to the public, online. They are building defamatory websites and posting defamatory comments online. While

initially the victims of the defamation may ignore the postings and websites, they are starting to take action more and more frequently. And kids and teenagers are getting into the act as well. When harassment occurs and young people are on both sides of the events, with a young person harassing another young person, it is typically called cyberbullying. (When an adult is on one side or another, it is typically called cyberstalking or harassment.)

Our kids need to know that the online services and ISPs will provide their identity pursuant to legal process. And they can be found and held responsible for what they say and do online. It's very important that we teach our children to understand accountability, online and offline. Schools can be very helpful here. Unfortunately, sometimes when cyberbullying occurs the schools get involved in trying to discipline the students for off-hours and off-premises activities, often to their detriment.

Off-School Web sites

Just as kids have circulated derogatory jokes and drawings of teachers over the generations, these digital kids circulate their jokes, insults, and drawings using the power of the Web, where they can be viewed by everyone. They then share the URL (Web address) of the site, so fellow classmates can appreciate their work. Often the URL ends up in the hands of a teacher. Teachers and administrators who are the target of the site report it, and threaten to file a lawsuit or to report it to the police. The school then feels compelled to do something. Typically the child is suspended or expelled, or college recommendations are withdrawn.
But several times the ACLU has taken these schools to court for disciplining a child for actions taken off-premises, and in most cases the school has lost the lawsuit. It can be a very costly mistake—a school system may have to pay $50,000 or more in damages when it exceeds its authority in this area. So what's a school to do? I would suggest they take their lead from a very experienced school superintendent.

A teenager in that high school, after getting angry with certain teachers and administrators, lashed out by posting some pretty vulgar and insulting things about them on a personal website. He wrote the site from home and posted it online. It wasn't posted on the school's server, but was available to everyone with Internet access once they had the URL. URLs of classmates' sites get passed around quickly, and many of the kids in the school accessed the site from the school's computers.

When the word got back to the teachers and administrators, they were understandably furious. They sought help from the police, who threatened to charge the teenager with harassment (but they wouldn't have been able to make that charge stick).

Everyone involved seemed to lose their head, but the superintendent managed to keep his. He recognized that this wasn't a school matter, and that the parents needed to be involved. He called in the parents, who were appalled and took this situation as seriously as they should have. Together they worked out a suitable apology and a way to handle the case without blowing it out of proportion. The press had a field day. This superintendent stood firm against the anger of the teachers and the pressures of the community. He was right.

Months later he shared something with me. He told me that he had met the young teenager at a school event, and the student apologized once again. He also thanked the superintendent for handling the situation with grace. The boy had acted out in anger, and hadn't thought about the consequences of his anger. Eventually, even the teachers came around. I was sorry my children were already out of high school—they would have benefited from attending a school system run by such a patient and wise administrator. We could use many more like him.
An even greater risk occurs when a student is targeting another student with cyberbullying tactics. They may post derogatory things about them online, pose as them in communications with others or postings online, change their passwords, hack into their accounts, take digital images of them and post those (sometimes in altered pornographic poses) using mobile phone cameras, digital cameras and video. The methods used by kids to harass each other are limited only by their limitless imaginations, bandwidth and tech skills.

The courts in the United States have reviewed several of the cases where the school has taken disciplinary action to protect its staff or the school itself from harassment and another student from cyberbullying, even if it occurs from outside of school. Most cases rule against the school, but some new ones are ruling in the school's favor on the basis that these matters affect the safety in the school itself. (Our WiredSafety.org cyberbullying and cyberharassment legal pages will launch soon, check back, or sign up for notice of our Web site alerts.)

What Can a School Do About This?

While taking disciplinary action against a student that does something outside of school hours and off school grounds may exceed a school's normal authority and land the school in legal hot water, doing so with the consent of the parties is not. Most schools have an acceptable use policy. And the smart ones have it signed by the parents and the students. It typically deals with what is and is not permitted use of the schools technology and computer systems. And, it is a legal contract binding the parents and the school (and the students themselves once they are of legal contracting age).

By adding a provision that covers dangerous or abusive actions by a student that directly affects another student, the school itself or its staff, the school now has authority to take appropriate action to deal with the dangerous or abusive conduct. It is the impact on the school, its safety and the safety and well-being of its staff and students that will trigger the school's authority, not whether the actions took place from a school computer within school hours. Laying out the problems and the impact of these problems on others at the school and the need to protect students, staff and the educational environment of the school is the place to start. Then, add an express consent to the school's taking action in the event it deems the matter to have an adverse impact on safety and the welfare of students, staff and the educational environment. It's that simple. But, as in all things legal, the devil is in the details.

School board attorneys, or special cyberspace attorneys expert in children's issues should be retained to draft and implement policies to enforce acceptable use polices and risks management programs. This is not an area for amateurs or "wanna-be lawyers." It's also not the time to cut and paste another school's acceptable use policy and use it as your own.

The school should conduct an audit of its technology uses and needs. It needs to know how the technology is being used currently, as well as the recommendation of the experts within the school. These experts should include, at minimum, the school safety officer, the school board attorney, the principal, disciplinary officer, technology lab instructors, IT department and the librarian or library media specialist. It is best to also include a student representative and a parent representative, guidance counselor and mental health professional.

Then do some strategic planning. What's on the horizon as far as new software applications and hardware installations? What is the five-year plan? Does the school even have a five-year plan? If not, what's the two-year plan? (If you don't have one of those, do not read further…find a professional to help you on more elemental things. You have serious problems.) Are their possible partners you can rely on? What about your computer suppliers? Your ISP? These companies have an amazing number of resources available to them to help schools. See what they have and don't be afraid to ask for their help.

Once you have a snapshot of what you are doing and what you plan to do, think about what you should be doing. Look to other schools for guidance as well as professional educational associations. Then, put your pen to paper (or you fingers to the keyboard J) and explain what you are now doing, what you will be doing and the rules. Once that is done, lay out the range of disciplinary actions that might be taken and the parameters. Use simple language that the students and non-techies can understand. When that's all done, run it by the lawyers to make sure you haven't done anything wrong and haven't left anything out. Then cross your fingers, hold your breath and wait.

I am interested in hearing from those you of who have been through this process, and would love to highlight your work and share your successes (publicly) and your disasters (anonymously). Drop me an e-mail. We're all in this together.

Sticks and Stones - Defaming Others Online

Sticks and stones will break their bones, but words will never hurt them—right? Wrong! While the First Amendment gives us the right of free speech, it does not give us the right to say false and horrible things about others. In the United States, someone whose reputation is damaged by a false statement made by another can sue that person for defamation. (Libel is when the defamatory statement is written, and slander is when it is spoken.) Under rare circumstances, such statements and the way they are delivered may rise to the level of cyberstalking or harassment, considered a crime in more than 46 states.

Unfortunately, since the advent of the Web, many are taking their grievances to the public, online. They are building defamatory websites and posting defamatory comments online. While initially the victims of the defamation may ignore the postings and websites, they are starting to take action more and more frequently. And kids and teenagers are getting into the act as well. When harassment occurs and young people are on both sides of the events, with a young person harassing another young person, it is typically called cyberbullying. (When an adult is on one side or another, it is typically called cyberstalking or harassment.)

Our kids need to know that the online services and ISPs will provide their identity pursuant to legal process. And they can be found and held responsible for what they say and do online. It's very important that we teach our children to understand accountability, online and offline. Schools can be very helpful here. Unfortunately, sometimes when cyberbullying occurs the schools get involved in trying to discipline the students for off-hours and off-premises activities, often to their detriment.

Off-School Web sites

Just as kids have circulated derogatory jokes and drawings of teachers over the generations, these digital kids circulate their jokes, insults, and drawings using the power of the Web, where they can be viewed by everyone. They then share the URL (Web address) of the site, so fellow classmates can appreciate their work. Often the URL ends up in the hands of a teacher. Teachers and administrators who are the target of the site report it, and threaten to file a lawsuit or to report it to the police. The school then feels compelled to do something. Typically the child is suspended or expelled, or college recommendations are withdrawn.

But several times the ACLU has taken these schools to court for disciplining a child for actions taken off-premises, and in most cases the school has lost the lawsuit. It can be a very costly mistake—a school system may have to pay $50,000 or more in damages when it exceeds its authority in this area. So what's a school to do? I would suggest they take their lead from a very experienced school superintendent.

A teenager in that high school, after getting angry with certain teachers and administrators, lashed out by posting some pretty vulgar and insulting things about them on a personal website. He wrote the site from home and posted it online. It wasn't posted on the school's server, but was available to everyone with Internet access once they had the URL. URLs of classmates' sites get passed around quickly, and many of the kids in the school accessed the site from the school's computers.

When the word got back to the teachers and administrators, they were understandably furious. They sought help from the police, who threatened to charge the teenager with harassment (but they wouldn't have been able to make that charge stick).

Everyone involved seemed to lose their head, but the superintendent managed to keep his. He recognized that this wasn't a school matter, and that the parents needed to be involved. He called in the parents, who were appalled and took this situation as seriously as they should have. Together they worked out a suitable apology and a way to handle the case without blowing it out of proportion. The press had a field day. This superintendent stood firm against the anger of the teachers and the pressures of the community. He was right.

Months later he shared something with me. He told me that he had met the young teenager at a school event, and the student apologized once again. He also thanked the superintendent for handling the situation with grace. The boy had acted out in anger, and hadn't thought about the consequences of his anger. Eventually, even the teachers came around. I was sorry my children were already out of high school—they would have benefited from attending a school system run by such a patient and wise administrator. We could use many more like him.

An even greater risk occurs when a student is targeting another student with cyberbullying tactics. They may post derogatory things about them online, pose as them in communications with others or postings online, change their passwords, hack into their accounts, take digital images of them and post those (sometimes in altered pornographic poses) using mobile phone cameras, digital cameras and video. The methods used by kids to harass each other are limited only by their limitless imaginations, bandwidth and tech skills.

The courts in the United States have reviewed several of the cases where the school has taken disciplinary action to protect its staff or the school itself from harassment and another student from cyberbullying, even if it occurs from outside of school. Most cases rule against the school, but some new ones are ruling in the school's favor on the basis that these matters affect the safety in the school itself. (Our WiredSafety.org cyberbullying and cyberharassment legal pages will launch soon, check back, or sign up for notice of our Web site alerts.)

What Can a School Do About This?

While taking disciplinary action against a student that does something outside of school hours and off school grounds may exceed a school's normal authority and land the school in legal hot water, doing so with the consent of the parties is not. Most schools have an acceptable use policy. And the smart ones have it signed by the parents and the students. It typically deals with what is and is not permitted use of the schools technology and computer systems. And, it is a legal contract binding the parents and the school (and the students themselves once they are of legal contracting age).

By adding a provision that covers dangerous or abusive actions by a student that directly affects another student, the school itself or its staff, the school now has authority to take appropriate action to deal with the dangerous or abusive conduct. It is the impact on the school, its safety and the safety and well-being of its staff and students that will trigger the school's authority, not whether the actions took place from a school computer within school hours. Laying out the problems and the impact of these problems on others at the school and the need to protect students, staff and the educational environment of the school is the place to start. Then, add an express consent to the school's taking action in the event it deems the matter to have an adverse impact on safety and the welfare of students, staff and the educational environment. It's that simple. But, as in all things legal, the devil is in the details.

School board attorneys, or special cyberspace attorneys expert in children's issues should be retained to draft and implement policies to enforce acceptable use polices and risks management programs. This is not an area for amateurs or "wanna-be lawyers." It's also not the time to cut and paste another school's acceptable use policy and use it as your own.

The school should conduct an audit of its technology uses and needs. It needs to know how the technology is being used currently, as well as the recommendation of the experts within the school. These experts should include, at minimum, the school safety officer, the school board attorney, the principal, disciplinary officer, technology lab instructors, IT department and the librarian or library media specialist. It is best to also include a student representative and a parent representative, guidance counselor and mental health professional.

Then do some strategic planning. What's on the horizon as far as new software applications and hardware installations? What is the five-year plan? Does the school even have a five-year plan? If not, what's the two-year plan? (If you don't have one of those, do not read further…find a professional to help you on more elemental things. You have serious problems.) Are their possible partners you can rely on? What about your computer suppliers? Your ISP? These companies have an amazing number of resources available to them to help schools. See what they have and don't be afraid to ask for their help.

Once you have a snapshot of what you are doing and what you plan to do, think about what you should be doing. Look to other schools for guidance as well as professional educational associations. Then, put your pen to paper (or you fingers to the keyboard J) and explain what you are now doing, what you will be doing and the rules. Once that is done, lay out the range of disciplinary actions that might be taken and the parameters. Use simple language that the students and non-techies can understand. When that's all done, run it by the lawyers to make sure you haven't done anything wrong and haven't left anything out. Then cross your fingers, hold your breath and wait.

I am interested in hearing from those you of who have been through this process, and would love to highlight your work and share your successes (publicly) and your disasters (anonymously). Drop me an e-mail. We're all in this together.

Bullying Prevention Resource Guide

FOR SCHOOLS, FAMILIES AND COMMUNITY PARTNERS
Key Facts & Statistics

More than half of children between the ages of 8 and 11 – and 70% of kids in the middle grades – say that bullying is a"big problem" at school.
Kaiser Family Foundation, 2001

Nearly 1.5 million students in grades 6-10 report being physically or verbally bullied at least once a week.
National Crime Prevention Council, 2003

Roughly one in three teenagers – and nearly half of 15- to 17-year-old girls – say they have been the victim of an online rumor, threatening messages or other forms of bullying via electronic communication.
Pew Internet & American Life Project, 2007

Only 30% of students who had witnessed or been the target of bullying said teachers intervened "often" or "always" –contrasted with up to 85% of teachers who described themselves as doing so.
Yorber & Kern, 2003

Among the small percentage of high school freshmen who said they had told an adult about witnessing or being the target of bullying, nearly two-thirds said the result was "nothing changed" or "things got worse."
National Association of Secondary School Principals, 2001

An in-depth study by the U.S. Secret Service of 37 school shootings between 1974 and 2001 found that in most cases, bullying played "a key role in the decision to attack."
U.S. Secret Service, 2001

Young people who bully are more likely to dislike and do poorly in school than other students, and are at higher risk for fighting, vandalism, substance abuse and other antisocial behavior. Chronic bullies seem to maintain their behaviors into adulthood. In one study, two-thirds of boys identified as bullies in grades 6-9 had at least one criminal conviction by age 24, and 40% had three or more arrests by age 30.

National Youth Violence Prevention Resource Center