



## Family Insider—Cyber Ethics

### Table of Contents

Family Insider .....1  
 Get Involved .....2  
 Ethics .....3  
 Did You Know? .....4  
 Commandments of Cyber Ethics .....4  
 Net Ethics & Intellectual Property ....5  
 Internet Safety Tip .....5  
 Operation i-SHIELD .....6



**“Developing the mind is important, but developing a conscience is the most precious gift parents can give their children.”**

*~John Gray*

Ethics is the system of moral principles by which we all live. Cyber ethics is simply the system of moral principals that apply to our online world. Acceptable behaviors on the Internet are very much the same as acceptable behaviors in our physical world and it is very important that we help our kids to clearly understand cyber ethics as they apply to online behavior and good citizenship.

Children learn very early in life not to take property that belongs to others, not to copy someone’s homework, and not to steal. Likewise, they learn about honesty, respecting others and the consequences of illegal or inappropriate behaviors. But, as they enter and interact in the cyber world, do they take those attitudes and behaviors with them?

Online activities such as hacking, phishing, and pharming are the online equivalents of breaking and entering; and online pirating or plagiarism are like stealing. A student who finds a key with a building’s address written on it would not likely try to use the key to enter that locked building; and most students wouldn’t even think of stealing a CD from a music store. But often they don’t associate those real-life behaviors with their online equivalents. Cyber bullying and harassment is a growing problem with students. And since the bullies either don’t see the impact their harassment is having on their victim, or just figure they won’t be caught, students continue to harass and degrade others online.

So what can you do to teach your child about cyber ethics?

Helping students learn about ethical behavior and how to make wise decisions is an ongoing process. Modeling



good cyber citizenship is the first step. Students sometimes find the lines between right and wrong are blurred when it comes to online behavior. That may be due to the lack of proper cyber ethics education, or they may become confused regarding right and wrong by what they see from their parents or other adults. Students who observe adults copying software or music for their own use, sending disrespectful e-mails or flaming conversations online, using company e-mail accounts or resources for personal use, or participating in other inappropriate or

*continued on page 2*

### NAC Tracks

Does your family discuss cyber ethics?

A: Yes

B: No


**Vote here**





## Cyber Ethics continued from page 1

unethical behaviors online, may deem those behaviors acceptable. In a phrase: monkey see, monkey do.

Here's what you can do. First, set a good example, both online and in the physical world. Talk with your kids about ethics. Give them examples of real-life situations and ask them how they would respond if they were confronted with parallel situations online. Be sure to discuss consequences for illegal or inappropriate behavior, both in their physical community and in the cyber world. It helps to practice making decisions responsibly and appropriately. 



## Get Involved—*Becoming More Visible in Your Child's Life*

Research shows that being actively involved in your child's life benefits them socially and academically, and creates children with higher self-esteem, less behavioral problems and better grades.


How you can become more positively involved in your child's life.:

- **Be a good role model** – Your kids really are watching what you are doing and saying!
- **Attend school functions, PTA meetings, and parent teacher conferences** – Educators do want greater parent participation! And attending events and conferences show your child that you care.
- **Provide encouragement and help your child with homework** – A “great job” or “way to go” will give your child confidence and encouragement to do well.
- **Reinforce your child's classroom lessons in your home** – Example: if they are learning about measurements, let them cook with you; if they are learning about computer security, go online with them and review what they've learned and how it applies to your family's computers. Help them practice making good decisions.
- **Volunteer at your child's school** – Schools encourage parent involvement and welcome parents as volunteers in the school and in the classroom.
- **Serve as an advocate for important issues** – Cyber bullying, Internet safety curriculum, drug abuse programs, etc.

In this month's newsletter we are focusing on cyber ethics and how important it is to model good behavior and teach your children about appropriate, ethical behavior, both in



their physical community and in their cyber community.

As always, i-SAFE is leading the way with a comprehensive cyber ethics program based on our current curricula offerings. Those same lessons already being used can be easily coordinated into cyber ethics curricula. More themed lessons such as respect, friendship, and responsibility will be added in the months to come. So stay tuned. Talk to your child's teacher to see what they are doing to address cyber ethics in the classroom. 



## ēth'iks – a set of principles of right conduct

An Internet search for the word ethics produces more than 100-million results; people's opinions as to what the word means seems to be as varied. There is the study of ethical systems, ethical and moral philosophy, and the concept of applied ethics.

Regardless of the ambiguous nature of ethics, you and I intuitively know the meaning of ethics as it relates to our lives, right? This is because, for the most part, applied ethics is part of our everyday lives; we know what we ought to do or not do in any given situation. Beginning with early childhood we have a set of customs and behaviors imposed on us by our immediate families and those around us. These influences help shape who we become and how we make decisions about right and wrong. Typically, the knowledge we gain through this development process is adequate to help us navigate the obstacle course of decision making that we encounter each day. As a society, though, we reinforce these values through education and law.

The development of the Internet has created a world that is seemingly separate from the physical world. Cyberspace exists as a direct result of the interconnected networks known as the Internet, which means it is completely connected to the world we live in. Since the World Wide Web so easily crosses territorial and cultural borders, it is difficult to regulate through law or to impose ethical guidelines on users.

The United States government has enacted laws to criminalise certain online behaviors, to protect users from predators, spammers, identity thieves, and hackers. Bills introduced in the U.S. Congress seek to hamstring the efforts of sex offenders who prey on children through the use of phony screen names and the use of social networking sites. Other legislation sought to divide the cyber world into separate spheres, with the intent of helping kids stay away from x-rated adult content sites. The dot-kid legislation created a designated address ending for kid-friendly sites but has received very little use. The so-called dot-xxx bill was met with fierce resistance from the pornography industry and was defeated.


At the same time in Europe, there is a move by several countries to regulate the Internet. One law would limit when potentially objectionable Internet advertisements can be shown, and to allow users the ability to not view the ad at all. The thought process here is that, just like with television, there are some advertisements that are not suitable for viewing at a certain time of day. These examples show that the decentralized nature of the Internet makes it



difficult for government to impose order and values on the Internet.

That's because a trip in Cyberspace is normally an individual experience. Therefore, users must bring their already learned set of ethics with them, and apply their real-life to their life online.

So, more than ever, education is key. Beginning at an early age and continually reinforced, students need to be taught they are part of a cyber community—just like their physical community—and there are rules, laws, and values to be learned and applied to both worlds. i-SAFE offers rich educational formats for K-12 students and for parents.

Through some trial and error, governments are learning what they can and can't regulate online. Behavior-based laws equip law enforcement to prosecute predators, scammers, and others who seek to capitalize on the openness of the Internet and the unsuspecting nature of its users. And governments are also learning that education is the best way to reinforce the values of our society. The ethical standards that have been honed throughout the years serve us well and will continue to do so on the Internet. Order and values begin with the individual who is part of a group. Transforming the world wild web into the World Wide Web means taking on the values of its users who more and more are learning to apply what they know and learn from Internet safety organizations like i-SAFE to create an appropriate online environment for everybody. 



## Did You Know?

### Internet Complaints

The IC3 (Internet Crime Complaint Center) working in partnership with the FBI and the National White Collar Crime Center, has issued national statistics in its 2006 report. Surprisingly, the most complaints (44.9%) are about auction fraud, compared to identity theft being only 1.6% of the complaints recorded, and credit/debit card theft fraud being 4.8%. To learn more about the IC3 statistics or to report fraud, go to [www.ic3.gov](http://www.ic3.gov).

### If a Voice Can Text

Texting and e-mailing are hard to do on the go, especially when driving. Now Jott.com is providing a new service by translating spoken words into text or e-mail messages. You simply dial a toll-free number, speak your information, and then forward it to an e-mail address or cell phone.

### Reward for Hackers?

The long awaited new iPhone finally hit the market last summer. Some of the excitement brought by this new superphone dwindled when it was realized that Apple set up a five-year contractual agreement so that iPhones would only work when connected through AT&T as a service provider.

So George Hotz, a New Jersey teen, found a way to unlock the iPhone so that it could get service from T-Mobile, allowing one more consumer option.

It seems that hacking of this product was not illegal. Hotz turned in a hacked phone to CertiCell and was rewarded with a trade of a new Nissan 350Z and three new 8 GB iPhones. He also has a consulting opportunity with CertiCell and a potential paycheck.

The question remains out there—is unethical behavior being rewarded, or is it simply ingenuity?

## Ten Commandments Of Computer Ethics

*Created by the Computer Ethics Institute*

1. Thou Shalt Not Use A Computer To Harm Other People.
2. Thou Shalt Not Interfere With Other People's Computer Work.
3. Thou Shalt Not Snoop Around In Other People's Computer Files.
4. Thou Shalt Not Use A Computer To Steal.
5. Thou Shalt Not Use A Computer To Bear False Witness.
6. Thou Shalt Not Copy Or Use Proprietary Software For Which You Have Not Paid.
7. Thou Shalt Not Use Other People's Computer Resources Without Authorization Or Proper Compensation.
8. Thou Shalt Not Appropriate Other People's Intellectual Output.
9. Thou Shalt Think About The Social Consequences Of The Program You Are Writing Or The System You Are Designing.
10. Thou Shalt Always Use A Computer In Ways That Insure Consideration And Respect For Your Fellow Humans.

© Copyright 1992 Computer Ethics Institute





## Net Ethics and Intellectual Property

In today's global, technology-driven society, net ethics are often overlooked by youth when it comes to online use of intellectual property.


Ask an American student this question, "Do you think it is ethical for someone to go into a jewelry store, pick up a ring that is displayed on the counter, and walk right out of the store with it?" Any student over the age of 5 will answer correctly – that the person is wrong for stealing the ring.

However, replace the words "jewelry store" with the word Internet. And talk about "music files" instead of a ring, and the student will probably give a very different answer. Results of an i-SAFE survey of high school students show that of the students who download music, 77% do so illegally. At 74%, the illegal downloading rate among middle school students isn't much better.

Sometimes it seems that there are almost as many reasons to justify their illegal behavior as there are students. Among the most popular: everything on the Internet should be free; that the music files are there for the taking; nobody gets hurt; artists are already rich enough; the chance of getting caught is nil; and everybody is doing it. Educators at all levels must recognize that net ethics, especially in regards to the use of intellectual property, cannot be isolated from general social behavior, and therefore is a topic that must become a part of everyday teaching and learning.



i-SAFE programs have demonstrated that education on responsible use of the Internet can raise significant awareness among students and positively change their behaviors. Based on a recent sampling of 10,000 U.S. students after receiving i-SAFE intellectual property curriculum, 55% say that they will never copy music for friends in the future, and 46% say they won't accept pirated music from their friends. 58% say they now realize people lose money when they illegally download music. And to further gauge the impact of education, of the 61% of students who say they regularly download music, more than half (51%) say they'll now pay or get permission to do so in the future.

Ethical dilemmas posed by the Internet will continue to face our youth. Education is key! 

## Internet Safety Tip—*Think Twice Before Forwarding E-mails*

Did you know that forwarding e-mails can put you and your friends at risk?


Forwarding is the act of sending a received e-mail message to others, usually without editing it. E-mails should not be indiscriminately forwarded for several reasons:

1. When you forward e-mail, you can be giving out personal information such as the e-mail address of the person who sent it to you, as well as any others in the original list of recipients.
2. Indiscriminate forwarding of e-mail can also be considered to be spamming. Make sure the e-mail you send has a point. If you have to forward something, make sure you know the complete contents of the e-mail including any attachments; and do not include the e-mail addresses of anyone else.
3. Once you forward an e-mail, the recipient may forward

it, too, which provides your e-mail address to strangers. Share this newsletter with your friends so they too will know how to safely forward e-mails.

If you want to send information that you received in an e-mail to a friend:

- Copy the specific content that you want to send on to your friend (highlight the text and then click "Ctrl C").
- Open a new mail message window.
- Paste the specific content into your new message (click in the body of the e-mail and click "Ctrl V").

Address and send your e-mail. 

### Results from last month's NAC Tracks:

Does your child use an online tutorial Web site?

Yes: 54% No: 46%

## Operation i-SHIELD Gains Momentum

Almost everybody, it seems, has seen one or more segments of the Dateline NBC series, “To Catch A Predator,” in which reporter Chris Hansen sensationally exposes an adult predator (on camera to a nationwide viewing audience) who shows up at a typical American bedroom community residence for the purpose of secretly and illegally having sex with a very adolescent (13 or 14 year old) “home alone” female or male the predator met and “groomed” on the Internet.

Dads, moms and kids are shocked to learn this “stuff” is going on right under their noses and that the predators, who they expected to be the usual suspects (such as convicted criminals and perverts who look like perverts), are really guys (young, middle aged and senior) with normal and even stellar personal backgrounds, credentials and identities.

So what can we do?

The affordable and “doable” answer is PREVENTION—eliminate victims and victimhood!

On the Internet, geographical boundaries are meaningless. A child living in a statistically “low-crime” area is just as vulnerable to online crimes and criminals as is a child living somewhere else—location doesn’t matter. All criminals, including predators and identity thieves, use the same strategies and tactics on the Internet. Therefore, prevention strategies and tactics to keep children safe must match those of the online criminals.


One particularly noteworthy prevention initiative designed to deal proactively and effectively with the omnipresent threat posed by online child predators is i-SAFE’s network of i-SHIELD Task Forces, called Operation i-SHIELD. Operation i-SHIELD is a growing nationwide network of independent i-SHIELD Task Forces, that



pursue a common goal—Internet crime prevention. The overarching purpose of Operation i-SHIELD is to provide federal, state, and local law enforcement professionals with an informal, multidisciplinary organizational framework in which they can work together, using i-SAFE’s vast array of Internet safety resources.

At present, there are 291 i-SHIELD Task Forces established in cities and counties throughout the United States. 1,202 law enforcement professionals have joined them for the purpose of sharing ideas, information and contacts, using i-SAFE Internet safety resources.

Does your community have an i-SAFE Task Force? One place we often see our task force members is at our local schools. Often, our school resource officers (SRO) become educators of Internet safety for our youth.

When you meet Operation i-SHIELD Task Force members, you can thank them for not only helping to make your local community safe, but for also helping to make the greater online community a safe place. 

The series of i-SAFE newsletters also includes the *i-EDUCATOR Times* and *Kewl Timez* (for students). We encourage you to read the others and ask you to use the main article to initiate discussion and action with your students and your community.

### About i-SAFE

Founded in 1998 and active in all 50 states, i-SAFE Inc. is the leader in Internet safety education. i-SAFE is a nonprofit foundation whose mission is to educate and empower youth to make their Internet experiences safe and responsible. The goal is to educate students on how to avoid dangerous, inappropriate, or unlawful online behavior. i-SAFE accomplishes this through dynamic K through 12 curriculum and community-outreach programs to parents, law enforcement, and community leaders. It is the only Internet safety foundation to combine these elements. [www.isafe.org](http://www.isafe.org)

To send comments or contributions to the newsletter staff, e-mail [news@isafe.org](mailto:news@isafe.org) or send “snail mail” to:  
i-SAFE Editor  
5900 Pasteur Court, Suite 100, Carlsbad, CA 92008

i-SAFE Inc. is designated a tax-exempt 501(c)(3) charitable organization by the U.S. Internal Revenue Service. i-SAFE Inc. is funded by the U.S. Congress through the Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, Department of Justice.