Online Privacy

A Tutorial for Parents and Teachers

Being a good cybercitizen

For the Internet to be the fun, enlightening, and safe place we all want it to be, everyone, adults and children alike, must be good cybercitizens. Essentially, that means bringing the same ethical, considerate, and careful behavior to the online world that you practice offline. Several important aspects to being a good cybercitizen include:

- **Cyberethics**—Respect the feelings, property, and rights of others online. Don’t harass others, plagiarize, or download music or video illegally.
- **Cybersafety**—Never agree to meet in person strangers you meet online (especially important for children).
- **Cybersecurity**—Make sure your computer has up-to-date security software/hardware to protect you and the people with whom you communicate online from viruses and other online threats.
- **Online addiction**—Be aware that when text messaging, playing online games, chatting, or other online activities become more important than friends, family, or schoolwork, it may indicate an addiction that should be addressed immediately.
- **Online privacy**—Protect your personal privacy online to avoid physical or financial jeopardy. Children should never provide personal or financial information online without the permission of a parent or other trusted adult. Parents and teachers should read and understand the privacy policy of any Web site children visit or join. They should also look for a privacy seal that ensures the good privacy practices of the Web site.

This tutorial focuses on the topic of online privacy risks and how to discuss them with your students and children.

Knowledge is power

Privacy and security protection requires information. *Online Privacy—A Tutorial for Parents and Teachers* has been prepared to arm you with information that will help you and your children or students enjoy the Internet safely. Use this guide as a starting point to teach kids how to stay safe online so that they understand how they can control the use of their personal information, take security measures to help ensure their safety, and protect their privacy.

We at TRUSTe, Symantec, and iKeepSafe believe that staying educated is the best way to stay safe online. That is why we are offering this guide free of charge. You may request additional copies of *Online Privacy—A Tutorial for Parents and Teachers* by visiting www.truste.org/parent_teacher_tutorial.php.

Table of Contents

Online privacy: Why it’s important 6

Managing your own privacy 8

Social networking and instant messaging 10

Help from the government 11

The role of seal programs 12

Technology helps protect privacy 14

Tools for teaching online safety 15

Additional resources 16

Glossary 17

Privacy rules for kids 19

EDUCATE

PRIVACY

Online privacy: Why it's important

Kids and teenagers today are among the most savvy of Internet users, spending hours every week online. While adults spend their time shopping, banking, and getting up-to-date news, kids are surfing the Internet for answers to homework problems, gaming, and socializing with peers. Recent surveys estimate that more than 90 percent of kids use computers, while 87 percent use the Internet—and those percentages continue to grow.*

The role of parents and teachers

As parents and teachers, you probably have a good understanding of when you should or shouldn't reveal personal information. Children, on the other hand, are often less aware of potential threats and less wary. Phishers may lure your child or student into providing sensitive information. Predators may prey upon them. Businesses may collect and sell their or your personal information without your knowledge. Your role as a parent or teacher is to protect your children or students from these threats by providing informed guidance and supervision on online privacy. While the roles of parents and teachers overlap, there are important differences:

Parents

- □ Make sure your children understand the importance of maintaining their, and your privacy.
- □ Tell your children what information they may and may not provide online.
- □ Make sure they know that they should never join a Web site or give out personal information without your specific permission.
- □ Never let your child join a Web site without examining the site and reading the privacy statement.
- □ Monitor their exchange of instant messages and email. If you see names you don't know, ask.
- □ Check their browsing history in the Internet browser to see which sites they've visited.
- □ Use parental controls to limit your child's access to objectionable or dangerous Web sites.
- □ Maintain an ongoing dialogue with older children, such as tweens and teens, about Internet use and safety when strict controls are not possible or appropriate.

*Pew Internet & American Life Project Teens and Parents Survey, Nov.–Dec. 2004.

Teachers

□ Make sure students are only using computers for authorized activities such as doing assignments, researching, or collaborating with classmates.

□ Monitor students' use of instant messaging or email to collaborate with classmates to ensure that they don't share personal information, either in or beyond the classroom.

□ Limit student access only to Web sites that you or your school approve.

□ Read and make sure students understand a Web site's privacy policy before letting them provide any information to that site.

□ Develop and post rules for classroom Internet usage, share those rules with parents, and inform parents when a student fails to follow the rules.

□ Discuss plagiarism and the consequences of getting caught.

Managing your own privacy

- **Web site privacy statements are there to protect you.**
- **Avoid Web sites without privacy statements.**
- **Don't give information to a Web site that doesn't protect your privacy.**

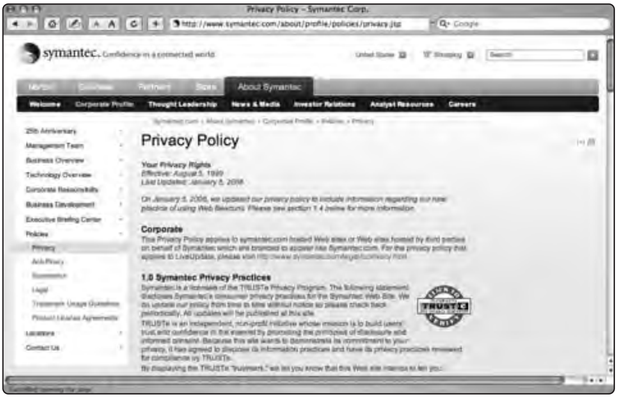
Before telling a Web site anything about yourself (such as your name, email address, physical address, phone number, likes or dislikes, favorite hobbies, financial information, etc.), look for the site's privacy statement. Parents or teachers and children should read the privacy statement together. We recommend that people, especially children, avoid any Web site that does not post a privacy statement.

Web site privacy statements

Privacy statements are the most important tools you can use to protect your privacy online. In a privacy statement, Web site owners tell you exactly what they will do with the personal information you give them. The privacy statement may be treated as a legally binding document. This means that a Web site owner must follow the privacy rules it says it will follow or face possible legal action.

There are four basic elements to any comprehensive privacy statement. Before you provide your personal information to any Web site, make sure it has these elements:

- **Notice**—Web sites should tell you what personal information they may collect and how they use it.
- **Choice**—Web sites should allow you to choose whether they can collect and use your information.
- **Access**—Web sites should give you the ability to access your personal information to correct any inaccuracies.
- **Security**—Web sites should provide reasonable security to protect your information from loss, misuse, or alteration.



Privacy Policy

Your Privacy Rights
Effective: August 5, 1999
Last Updated: January 5, 2006

On January 5, 2006, we updated our privacy policy to include information regarding our new practice of using Web Beacons. Please see section 1.4 below for more information.

Corporate
This Privacy Policy applies to symantec.com hosted Web sites or Web sites hosted by third parties on behalf of Symantec which are branded to appear like Symantec.com. For the privacy policy that applies to LiveUpdate, please visit http://www.symantec.com/legal/liveupdate/privacy.html

1.0 Symantec Privacy Practices
Symantec is a licensee of the TRUSTe Privacy Program. The following statement discloses Symantec's consumer privacy practices for the Symantec Web Site. We do update our policy from time to time without notice so please check back periodically. All updates will be published at this site.

TRUSTe is an independent, non-profit initiative whose mission is to build users' trust and confidence in the Internet by promoting the principles of disclosure and informed consent. Because this site wants to demonstrate its commitment to your privacy, it has agreed to disclose its information practices and have its privacy practices reviewed for compliance by TRUSTe.

By displaying the TRUSTe "trustmark," we let you know that this Web site intends to let you:

Privacy statement content

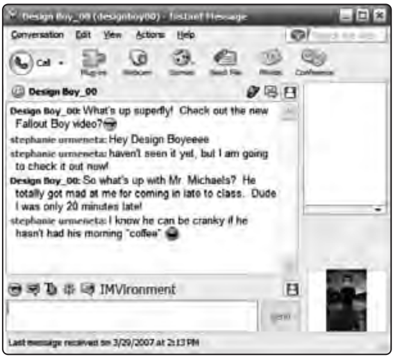
A Web site's privacy statement should provide the following information that you can read and use to make an informed decision about whether or not you want to entrust your personal information to the Web site.

- **Registration process**—A description of how the registration process works on the Web site.
- **Special features**—Special services the site provides, such as email, chat, discussion groups, and newsletters and how the personal information needed for those services is collected, managed, and used by the site.
- **Parental review of information**—For Web sites directed at children, how parents can review, change, or delete the information that such a Web site has gathered about their children.
- **Co-branding**—When a Web site has business agreements with other companies and information about the site's users is disclosed to those companies, the site must disclose what business the other company is in, how it uses the information, and whether the company agrees to maintain the confidentiality of the information.
- **Links to other sites**—Other Web sites that may be reached by clicking a link from the Web site. Any personal information given to those sites is treated in accordance with those other sites' privacy statements.
- **Cookies**—How the Web site uses cookies (which memorize your Internet address).
- **Contact information**—How you can get in touch with the Web site owner by email, postal mail, or phone if you have any questions about the site's privacy policy.

Social networking and instant messaging

Social networking Web sites and instant messaging are very popular among kids, and both pose some special privacy issues. Social networking sites such as MySpace, Friendster, Xanga, YouTube, and Facebook provide a place for them to get together online with existing and new friends. When used carelessly, however, these sites can expose children to identity theft and predators. Before allowing your child to join a social networking site, take these privacy precautions:

- To join a social networking site, a child must create a profile. Remind children not to provide personal information (real name, age, location) in a profile.
- Once they've joined a site, children can create their own Web page. Again, make sure they don't post identifying personal information on that page, that their page is private, and that they limit access only to invited friends.
- Read and understand the site's privacy policies.
- Read and understand the information for parents that most social networking sites provide.



Design Boy_00: What's up superfly! Check out the new Fallout Boy video?

stephanie urmeneta: Hey Design Boyeeee

stephanie urmeneta: haven't seen it yet, but I am going to check it out now!

Design Boy_00: So what's up with Mr. Michaels? He totally got mad at me for coming in late to class. Dude I was only 20 minutes late!

stephanie urmeneta: I know he can be cranky if he hasn't had his morning "coffee"

Last message received on 3/29/2007 at 2:13 PM

Instant messaging or "chat" enables kids to engage in online conversations via text or audio/video. It may be part of a social networking Web site or a service offered by Internet service providers or Web portals. Instant messaging also presents privacy concerns and warrants precautions:

- The Web site that includes the instant messaging service should provide a tutorial on how its service works, who has access to the chat conversation, and how it protects a user's identity. If it doesn't, contact the Web site and ask.
- Children should not participate in chat rooms with strangers. Make sure you know if your children are chatting on a private network with friends, or if there are strangers in the conversation. Tell them to leave any chat room that includes someone they don't know, and to tell you immediately.
- Instant messaging services provide a history of messages sent and received. To find the history, open the instant messaging application, and locate the history tab on the main application window or in the application preferences. If the history function is activated, simply click the tab to see the names of people your child has been messaging and to read the messages. If the history function is not activated, click it to activate it.
- Instant messaging services ask users to create a personal profile. Make sure your child doesn't include any identifying information in that profile.

Help from the government

Children’s Online Privacy Protection Act (COPPA)

In 1998, Congress passed a law establishing new rules to make sure that kids’ privacy is protected while they are online. As part of COPPA, Web sites directed at children or those that collect information from kids under age 13 must abide by the following rules:

- Web sites must post and provide easy access to a privacy statement that specifies how information is collected and used, including:
  - What personal information is collected (such as name, address, and hobbies)
  - Whether the collected information will be shared with third parties
  - Where to contact someone at the Web site who can answer any questions you may have
- Web sites must get verifiable parental consent before gathering, using, or giving out a child’s personal information (with some exceptions).
- Web sites must notify parents if they change how personally identifiable information is gathered and used, and get their new consent for the changes.
- Web sites must give parents access to review all personal information collected about their children.
- Web sites must, at any time, allow parents to opt out of future collection or use of information about their children.

The Federal Trade Commission (FTC) Act

The FTC Act is a law that gives the FTC the power to prevent unfair and deceptive business practices. Under this Act, if a Web site posts a privacy statement and then violates its posted policy, the FTC is empowered to take legal action against the site’s owners.

If a Web site does not abide by its posted privacy statement, it may be subject to legal action initiated by the FTC or state attorneys general. Web sites directed at children under age 13 are legally required to protect the privacy of children under the rules of COPPA. If you believe a children’s Web site is not following the rules of COPPA, contact the FTC or your state’s attorney general immediately. You can contact the FTC at www.ftc.gov/ftc/contact.shtm.

RULES

The role of seal programs

- **Ensuring Web sites secure your personal information.**
- **Protecting your child's privacy.**

Many Web sites use third-party services to accredit good practices. Once certified, the Web site is awarded a seal to display on its pages. Look for seals when making purchases or providing personal information to help ensure your safety. There are four main categories of seals.

- **Reliability seals** vouch for the identity of the company. They typically validate the mailing address of the company, its telephone number, and email addresses. These seals simply signify that the company is what it says it is.
- **Security seals** validate that a company has Secure Sockets Layer (SSL) protection for the transmission of sensitive data via Web forms. Look for the "lock" at the bottom of the browser window and the "https://" in the address bar—these indicate that while you are entering and submitting data to the Web site, criminals cannot intercept it.
- **Vulnerability seals** signify that a third party scans the site daily, weekly, or monthly looking for common security vulnerabilities that could be exploited by hackers.
- **Privacy seals** mean that a company respectfully uses the personal information you provide. Privacy seals require companies to undergo an extensive certification process that exposes internal data collection and usage processes. Programs also offer ongoing monitoring, and you can file a complaint with the program issuing the seal if you feel there has been misconduct.

The TRUSTe Privacy Seal

You may have seen the TRUSTe Privacy Seal or the TRUSTe Children's Privacy Seal on many of your favorite Web sites. These privacy seals mean that a Web site is dedicated to protecting your privacy and that you have the ability to control how your personal information is used by that Web site.

TRUSTe
CERTIFIED PRIVACY

A Web site that displays the TRUSTe Privacy Seal or the TRUSTe Children's Privacy Seal must have a privacy statement that tells you what the Web site does with the personal information you provide. The TRUSTe seal on a Web site means that the site will provide notice, choice, access, and security. The privacy statement can be reached by clicking a link from the site's home page or by clicking the privacy seal directly.

The TRUSTe Children's Privacy Seal is a seal for Web sites that are directed at children under age 13 or "general audience" sites that have special areas that collect personal information from such children. Any Web site displaying the TRUSTe Children's Privacy Seal must:

- Adhere to the privacy principles of notice, choice, access, and security
- Get verifiable parental consent before collecting personally identifiable information from a child
- Allow a parent to access and delete a child's personal information at any time

The TRUSTe seal on a Web site means that the site can be trusted to abide by the statements it makes in its privacy statement. This is because TRUSTe—a nonprofit, third-party oversight program—regularly monitors Web sites' adherence to their privacy statements and has the power to enforce compliance with its program.

Enforcement—you can help

TRUSTe provides a way for you to report privacy violations, so it can help you resolve your complaint with any Web site displaying the TRUSTe seal. If you believe your or your child's privacy has been violated on a Web site displaying the TRUSTe seal, we encourage you to contact TRUSTe directly by registering a complaint on the TRUSTe's Watchdog complaint form at www.truste.org/watchdog.

Technology helps protect privacy

There is more that you can do to protect yourself, your information, and your computer against those who don't play by the rules. Computer technology today is sophisticated, and so are online threats. For example, computer viruses can destroy your data, and spyware and phishing schemes can steal your personal and financial information. These and other threats are difficult to recognize without Internet security software, such as that offered by Symantec, the maker of Norton™ software.

Internet security software

We recommend that you protect your computer, at a minimum, with antispyware, antivirus, and firewall software, as well as backup software to protect against data loss. These can be found in most Internet security suite software packages. But comprehensive Internet security software provides protection against a broader range of known online threats:

- **Antivirus** protects your computer and your files against destructive viruses.
- **Antispyware** protects your computer from spyware that scammers place on the computer to steal your identity and to monitor transactions so they can steal your personal and financial data.
- **Antiphishing** recognizes and blocks fake or "phishing" Web sites, which mimic the appearance of legitimate Web sites and attempt to get you to give them personal or financial information.
- **Web site authentication** verifies that that the Web sites you visit are really what they appear to be.
- **Transaction security** monitors your online transactions to protect against identity theft.
- **Firewalls** block intruders before they enter your system.
- **Email scanning** helps ensure that the email and attachments you receive don't include spyware, viruses, or anything that can steal or destroy your personal information.
- **Automatic updates** help ensure that your information is protected from the latest threats.
- **Backup** protects against data loss.

For more information about all the ways Internet security software can protect your computers and networks at school and at home, visit www.norton.com.

Parental controls

When it comes to protecting children from dangerous Web sites, both parents and teachers can take advantage of the parental controls that are built into Internet browsers and the more rigorous parental controls that come with Internet security software. You can choose which Web sites children can or can't visit, and what type of content they can or can't view. It is a simple way to steer younger children away from dangerous or objectionable Web sites.

Tools for teaching online safety

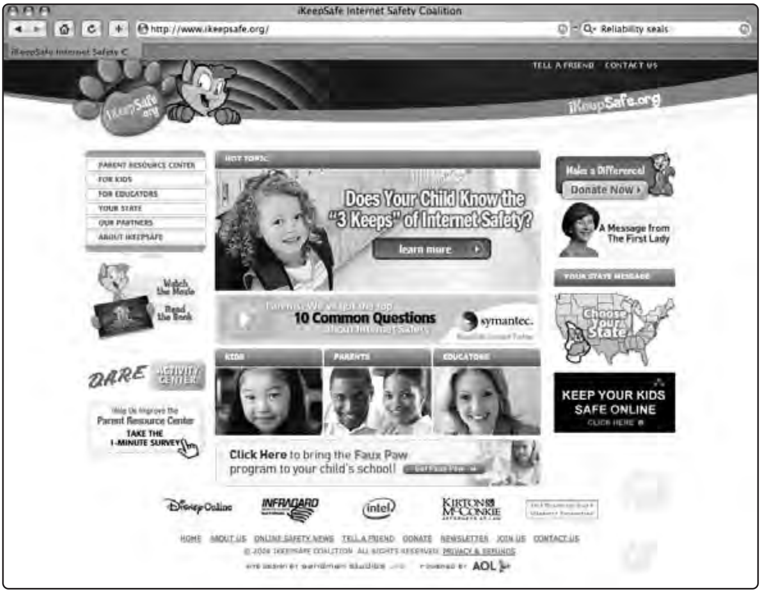
Many Web sites provide resources for teaching and learning about Internet safety, including governmental, nonprofit, and commercial Web sites. One of the most widely used and respected is iKeepSafe.org.

Three new tutorials at iKeepSafe.org, created in partnership with Symantec, help parents learn how to keep their children safe and solve the common problems that youth face online:

- *10 Actions Every Parent MUST Take*
- *What You Need to Know About Social Networking Sites*
- *What You Need to Know About Cyber-Bullying*

The iKeepSafe.org Web site offers Internet safety resources to teachers, parents, and children. It teaches children to safely navigate the Internet through a virtual playground. It uses an animated icon/mascot named Faux Paw the Techno Cat to teach children the importance of protecting personal information and avoiding inappropriate places on the Internet. Faux Paw's adventures in storybooks, an animated video download, and educational games all help kids learn about online safety. Educational materials, including worksheets and tests, are also available for parents and educators.

iKeepSafe.org is produced by the Internet Keep Safe Coalition, a broad partnership of governors and/or first spouses, crime prevention organizations, law enforcement agencies, foundations, and corporate sponsors dedicated to keeping children safe online. To take advantage of iKeepSafe's resources, visit www.iKeepSafe.org.



Additional resources

CyberAngels (www.cyberangels.org) describes itself as "your cyber neighborhood watch." The organization finds and reports illegal material online, educates families about online safety, works with schools and libraries, and shares basic Internet tips and help resources.

Family Resources (www.norton.com/familyresources) is a Web site produced by Symantec that helps parents provide guidance to their children who are using the Internet. Its goal is to provide parents with the information they need to keep their children and computers safe online and to help parents make sure that their children are good cybercitizens

Federal Trade Commission's Kidz Privacy site (www.ftc.gov/bcp/conline/ edcams/ kidzprivacy/index.html) is an educational Web site produced by the FTC surrounding the enactment of the Children's Online Privacy Protection Act (COPPA). This site offers guidance to parents and children as well as Web site operators on the do's and don'ts of children's online privacy.

GetNetWise (www.getnetwise.org) is a resource for families and caregivers to help kids have safe, educational, and entertaining online experiences. The Web site includes a glossary of Internet terms, a guide to online safety, directions for reporting online trouble, a directory of online safety tools, and a listing of great sites for kids to visit.

OnGuard Online (www.onguardonline.gov) maintained by the FTC, provides practical tips from the federal government and the technology industry to help you stay on guard against Internet fraud, secure your computer, and protect your personal information. The site offers tutorials, videos, and even quizzes to keep you in the know.

Top Ten Technical Questions (www.ikeepsafe.org/iksc_partners/symantec/ 10_questions/ Assets/TenCommonQuestions.pdf) is a list of the technical information that parents and teachers must know to keep kids safe online. Prepared by Symantec and iKeepSafe, it is especially valuable for parents and teachers without extensive technical knowledge, and for the technically aware, it provides a good refresher.

Wired Kids (www.wiredkids.org) is the official North American site of UNESCO's Innocence in Danger program. The site is under the direction of Internet lawyer and children's advocate Parry Aftab. Its mission is to allow children to enjoy the vast benefits of the Internet while at the same time protecting them from cybercriminals. The Web site will soon host a parent registry, allowing quickly accessible and verifiable parental consent.

Glossary

Blogs and Message Boards—These are areas on Web sites where you can post public messages. If you use your personal information to send messages, people who read your post can respond to you using your personal email address, or use the personal information you include to learn even more about you. Some Web sites offer the option to remain anonymous when participating in a blog or message board.

Chat Room—Online meeting places where you can talk to people by typing messages online. Typically, everyone participating in the chat sees your message. When you register for chat rooms, you may be asked for personal information. Don't give any that will endanger you.

Children's Online Privacy Protection Act (COPPA)—COPPA is a law that prescribes a set of rules meant to protect children's privacy online. One of these rules requires Web sites to get "verifiable parental consent" before accepting any personal information from children under the age of 13.

Cookies—Information placed in your computer's hard drive when you visit a Web site. Cookies allow the site to identify your computer the next time you visit. Cookies cannot identify you personally unless you have given your personal information to the Web site through a registration process or other means.

Opt-in—A Web site's request for permission and express consent before using any of your personal information. You must click a specific box if you want to allow the Web site to use your personal information (for example, to send you special offers through email).

Opt-out—A Web site's option to prevent it from using your personal information in any way. Usually you must click a specific box when prompted to enter your personally identifiable information.

Personally Identifiable Information (PII)—Any information or combination of information that allows a Web site to contact you and identify you as a specific individual. This information can include your full name, email address, or phone number.

Phishing—A growing problem in which criminals send out spam or pop-up messages to lure victims into sharing their personal and financial information on fake Web sites. Often phishers disguise themselves as well-known businesses and set up fake Web sites.

Social Networking Web Sites—Web sites that are popular with kids (especially teens). Some popular social networking sites are MySpace, Friendster, Xanga, YouTube, and Facebook. They provide a place for kids to get together online with existing and new friends. They require users to create a personal profile. Make sure that profile doesn't include personally identifiable information such as your last name, phone number, address, or school.

Spam or Scam Email—Spam refers to unwanted, unsolicited email. Scam email attempts to lure you into providing personal information to thieves, or it sends attachments that may include spyware or viruses.

Spyware—A program that can be installed on your computer from a remote location to steal your personal or financial information or to monitor your online transactions so that it can capture your information. It can be detected and removed by Internet security software.

Third-Party Ad Servers—More commonly known as the companies that place banner advertising on Web sites, third-party ad servers are not usually the owners of the Web site on which they advertise. The original Web site's privacy policy does not extend to the advertiser.

Verifiable Parental Consent—The permission slip for the Internet—parents must give permission to Web sites that want to collect personal information from children under the age of 13. Parents must be able to identify themselves as an adult and as the child's parent, using verifiable means such as a credit card number or a signed letter.

Virus—A software program designed to spread from one computer to another and to interfere with computer operations. Viruses may corrupt or delete data, use your email program to spread themselves to other computers, or even erase everything on your hard disk. They are most easily spread by attachments in email messages or by instant messaging messages. Don't ever open an email attachment unless you know who it's from and you are expecting it.

Privacy rules for kids*

Follow these rules when going online—or create your own Web contract between you and your child.

I can go online at __________ (Time of day) for __________ (How long).

□ It's OK □ not OK for me to go online without a parent.

□ I understand which Web sites I can visit and which ones are off limits.

□ I will not give out information about my family or myself without permission from my parents.

□ My password is my secret. I will not give it to anyone.

□ I will never agree to meet an online pal, or send my picture without permission from my parents.

□ I know an advertisement when I see one. I also know that animated or cartoon characters aren't real and may be trying to sell me something or get information from me.

□ I will follow these same rules when I am at home, in school, at the library, or at a friend's house.

□ I will remember to:

Keep safe: I keep safe my personal information—all of it! I never give my real name, address, phone number, the name of my school, or a picture of myself to anyone online.

Keep away: I keep away from Internet strangers—no matter what they tell me, because I have no way of knowing who they really are. I don't talk with them online, and I never meet them face to face.

Keep telling: I keep telling my parents or a trusted adult about everything I see on the Internet. I always tell them when something makes me uncomfortable.

An agreement about using the Internet between:

Child's Name	Parent's/Guardian's/Teacher's Name
Child's Signature	Parent's/Guardian's/Teacher's Signature
Date	Date

*Reprinted with permission from the Federal Trade Commission and the National Association of Attorneys General.

Internet Keep Safe CoalitionSM
4607 N 40th St.
Arlington, VA 22207
Tel: +1 703 536 1637
www.iKeepSafe.org

The mission of the Internet Keep Safe Coalition (iKeepSafe) is to empower parents, educators, and caregivers to teach children the safe and healthy use of technology and the Internet. Formed as an international partnership of governors and first spouses, crime prevention organizations, law enforcement agencies, foundations and corporate sponsors, iKeepSafe teaches basic rules of Internet safety via their website, as well as a variety of books, games, videos and educational materials. iKeepSafe's animated mascot, Faux Paw the Techno Cat, shows children in a fun way how to protect their personal information, to surf safely, and how to deal with cyber-bullying etc. For more information visit www.ikeepsafe.org http://www.ikeepsafe.org.

Symantec Corporation
20300 Stevens Creek Blvd.
Cupertino, CA 95014
Tel: +1 408 517 7883
www.norton.com

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world. The company helps customers protect their infrastructure, information and interactions by delivering software and services that address risks to security, availability, compliance and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

TRUSTe
685 Market Street, Ste. 270
San Francisco, CA 94105
Tel: +1 415 520 3400
www.truste.org

About TRUSTe
TRUSTe helps consumers and businesses identify trustworthy online organizations through its Web Privacy Seal, Email Privacy Seal and Trusted Download Programs. An independent, nonprofit organization celebrating its 10th anniversary in 2007, TRUSTe certifies more than 2,000 Web sites, including the major internet portals and leading brands such as AOL, Microsoft, IBM, Oracle, Intuit and eBay. TRUSTe resolves thousands of individual privacy disputes every year. To learn more about internet privacy visit www.truste.org.

10/07