Protecting Children Online

Child Guidance
Copyright © Texas Education Agency, 2012. These Materials are copyrighted © and trademarked ™ as the property of the Texas Education Agency (TEA) and may not be reproduced without the express written permission of TEA, except under the following conditions:

1) Texas public school districts, charter schools, and Education Service Centers may reproduce and use copies of the Materials and Related Materials for the districts' and schools' educational use without obtaining permission from TEA.
2) Residents of the state of Texas may reproduce and use copies of the Materials and Related Materials for individual personal use only, without obtaining written permission of TEA.
3) Any portion reproduced must be reproduced in its entirety and remain unedited, unaltered and unchanged in any way.
4) No monetary charge can be made for the reproduced materials or any document containing them; however, a reasonable charge to cover only the cost of reproduction and distribution may be charged.

Private entities or persons located in Texas that are not Texas public school districts, Texas Education Service Centers, or Texas charter schools or any entity, whether public or private, educational or non-educational, located outside the state of Texas MUST obtain written approval from TEA and will be required to enter into a license agreement that may involve the payment of a licensing fee or a royalty.

For information contact: Office of Copyrights, Trademarks, License Agreements, and Royalties, Texas Education Agency, 1701 N. Congress Ave., Austin, TX 78701-1494; phone 512-463-7004; email: copyrights@tea.state.tx.us.
Most people spend their time online:
• Posting a video from mobile devices
• Building online profiles
• Texting each other from their mobile devices
• Creating alter egos in the form on online avatars
• Connecting with friends online they don’t see regularly in person
• Sending photos to friends
• Broadcasting what they are doing to hundreds of people

U.S. Internet user on average spends 32 hours on Internet per month. How much time do you spend on the Internet? Were you surprised to learn these facts about how people spend their time on the Internet?
It is parents and caregivers responsibility to determine safeguards to prevent misuse and abuse of technology and media with children. What are parents and caregivers biggest concerns?

Inappropriate conduct-The online world can feel anonymous. Children sometimes forget that they are still accountable for their actions.

Inappropriate contact-Some people online have bad intentions, including bullies, predators, hackers, and scammers.

Inappropriate content-Parents may be concerned that children could find pornography, violence, or hate speech online. Parents can reduce these risks by talking to their children about how they communicate—online and off—and encouraging them to engage in conduct they can be proud of.
Children, Parents, and Video Games

Parental controls might include:
• Game Rating Restrictions
• Disabling Internet Access
• Time Limits
• Profiles
• In-game Purchase Restrictions

Video games have potential uses and management of technology, media, and resources to foster healthy child development.

Children play video games and as a parent or caregiver, you have ideas about what’s right for them when they do. Fortunately, tools like game ratings and parental controls can help you learn about the games children want to play — and help you make sure they’re playing according to your rules. That includes knowing how to make children can’t access online features if you don’t want them to. Regardless of the limits you set or the tools you use, talk to your children about them.

For many families, video games are a part of everyday life. Many games allow players to talk and play with other people — or buy more content right from the console or game. And plenty of games are designed with a grown-up audience in mind. That’s why it’s important to find out your parental control options.

Depending on the system, parental controls might include:

**Game Rating Restrictions:** This setting lets you decide which games can be played on a console or handheld gaming device based on the rating from the Entertainment Software Rating Board (ESRB). For example, you might set the system to allow games Rated E for Everyone to be played, but not games rated Teen or above.
Disabling Internet Access: This setting can prevent your children from accessing online features. For example, some systems include parental controls that allow you to mute or disable online chat, which might include profanity or bullying by other players. Some systems that offer online gaming also give parents the ability to approve friend requests or create approved lists of friends their kids can play with or talk to.

Time Limits: Some game systems let you set days and times your children can play, and for how long.

Profiles: Some systems let you create multiple profiles with different settings for each. So while your password-protected profile might allow you to play any game, your nine-year-old's profile might be limited to games rated E for Everyone. If your system doesn’t have profiles, you may have to reset the preferences each time you play.

In-game Purchase Restrictions: Sometimes you can buy downloadable games or downloadable content with the credit card tied to your account. But in most cases, you can set a password to restrict those purchases.
Along with using parental controls to set limits, think about what kind of games you want your children to play. That’s where game ratings come in. Video games have their own rating system from the ESRB. Ratings, printed right on the game box — or included at online storefronts for games downloaded directly to a game console — include:

**Age Ratings:** On the front of most game boxes, age rating symbols (Early Childhood to Adults Only 18+) give you an idea of the ages the game may be appropriate for.

**Content Descriptors:** On the back of the box, the content descriptors detail game elements — like violence, sex, language, and gambling — that may have triggered a particular rating.

**Rating Summaries:** If you’re looking for more information, check a game’s ESRB rating summary, a detailed description of key content. Rating summaries aren’t printed on the box, but you can look them up for most games at [esrb.org](http://esrb.org) or using the ESRB’s free mobile app. Games that are available only as a download through a console or handheld storefront do not get rating summaries.

Other organizations offer even more detailed information on game content. For example, Common Sense Media has game reviews, including recommended ages, at [commonsensemedia.org/game-reviews](http://commonsensemedia.org/game-reviews).
Online Rating Notice: If a game is online-enabled, it will include the notice, "Online Interactions Not Rated by the ESRB." That tells you that players could be exposed to chat — text, audio, or video — or other types of user-generated content that aren’t part of the game’s rating.
Mobile Game Apps

Parents can protect children by:
• Checking the rating system
• Phone settings
• Location sharing

If you have a smart phone or another mobile device with internet access, like a tablet or music player, you’re probably familiar with apps. The Android, Apple, Microsoft, and BlackBerry mobile operating systems, as well as some online retailers, have online app stores. But since not all apps are free, you may have to provide a credit card number to set up an account. Online mobile app stores and most smartphones have controls for parents to manage childrens’ purchase and use of apps.

**App ratings:** Some app storefronts have developed their own content ratings for the apps they offer. Others use a *rating system* developed by CTIA-The Wireless Association and the ESRB that’s based on the ESRB’s game ratings and lets developers get appropriate ratings for their apps. Some parental controls rely on content ratings to screen out apps that may be inappropriate for children.

**Phone settings:** You may be able to restrict content by age rating, or require a password for in-app purchases and app downloads. Check with your mobile provider.

**What some apps may allow:**

**In-App Purchases:** Some developers offer app users the ability to buy more content within a game. For example, you might be able to buy virtual currency from a game to buy virtual extras for an online world or avatar. Or you might be able to pay to upgrade to a premium version of a game. Usually, you’re billed for in-app purchases through the app store. Many devices have
settings that allow you to block in-app purchases or require a password before they can be made.

**In-App Advertising:** Ads running inside an app may allow you to call phone numbers directly or visit websites appearing in the ad. Some app descriptions tell you if an app is or isn’t ad-free.

**Location Sharing:** Some mobile games and apps and newer handheld gaming devices use a player’s location and might broadcast it to others. Many phones and devices let you turn this feature off.
For younger tweens, parental control—including filtering and monitoring tools—can be effective. However, many middle school children have the technical know-how to find a way to get around them. If children aren’t already using the Internet for their homework, this is when they’re likely to start. It’s also when they can discover resources for hobbies and other interests. Many tweens are adept at finding information online. That’s often helpful to the rest of the family, but they still need adult guidance to help them understand which sources are trustworthy.
Talk to the Children

Parental controls are a great tool, but they’re no substitute for talking to the children about the games they are playing.

Parental controls are a great tool, but they’re no substitute for talking to the children about:

• what games and apps they are playing or using
• what your family has decided is okay. Are there limits on what they can play, or when and how long they can play?
• who it’s okay to play games with online
• why it’s important not to share personal information, like their address, school, or plans for the weekend
• how to deal with inappropriate online behavior by another player. You may be able to block the player, or notify a game’s publisher or online service.

Another good idea: keep your computer or game system in a common area. That opens the door to ask questions and have conversations on the spot. For more, check out the ESRB’s Family Discussion Guide at esrb.org.
Child Identity Theft

• receive bills or notices for products or services you didn’t purchase or incur, including medical care
• be turned down for government benefits because the benefits are being paid to another account using your child’s Social Security number
• receive a notice from the IRS saying the child didn’t pay taxes on income or that the child’s Social Security number was used on another tax return.

Several signs can tip you off to the fact that someone is misusing your child's personal information and committing fraud. For example, you or your child might:

• receive bills or notices for products or services you didn’t purchase or incur, including medical care
• be turned down for government benefits because the benefits are being paid to another account using your child’s Social Security number
• receive a notice from the IRS saying the child didn’t pay taxes on income or that the child’s Social Security number was used on another tax return.
Check for a Credit Report

Contact each of the three nationwide credit reporting companies:

- Equifax: 1-800-525-6285
- Experian: 1-888-397-3742
- TransUnion: childidtheft@transunion.com

If you suspect that your child’s information may be at risk, check whether your child has a credit report by contacting each of the three nationwide credit reporting companies:

Equifax: 1-800-525-6285
Experian: 1-888-397-3742
TransUnion: childidtheft@transunion.com

Ask them to search using your child’s name and Social Security number; if nothing turns up, ask for a so-called manual search using just your child’s Social Security number.

If there is a credit report for your child, follow up with each credit reporting company. You’ll need to provide proof that your child is a minor, and that you are the parent or legal guardian.

Ask each company to remove all accounts, account inquiries, and collection notices from any file associated with your child’s name and Social Security number.
If you know that your child’s identity is being misused, call one of the credit reporting companies and ask for a fraud alert on your child’s credit report:

**Equifax** 1-800-525-6285  
**Experian** 1-888-397-3742  
**TransUnion** 1-800-680-7289

That company will contact the others, and shortly, all three will have placed fraud alerts on any reports associated with your child’s name or Social Security number. These alerts are in force for 90 days.

Next, file a report with the FTC. Do it at [ftc.gov/complaint](http://ftc.gov/complaint) or by calling 877-438-4338. If the fraud relates to medical services or taxes, you might need to file a police report, too.

Finally, contact every company where your child’s information was misused. Ask each to close the fraudulent account and flag it to show it resulted from identity theft.
When Your Child Turns 16

It’s a good idea to check whether your child has a credit report close to the child’s 16th birthday.

You can take some steps to protect your child’s identity from misuse:

• Keep all documents that show your child’s personal information locked up.
• Don’t share your child’s Social Security number unless you know and trust the other party. Ask why it’s necessary and how it will be protected. Ask to use another identifier, or at the very least, the last four digits of the Social Security number.
• Shred all documents that show your child’s personal information before throwing them away.
• Be pro-active in the face of certain personal circumstances, say an adult in financial hot water who might “adopt” a child’s identity to start over; a lost wallet or stolen purse that had your child’s Social Security card; a break-in at your home; or a notice that your child’s information was compromised in a data breach.

It’s a good idea to check whether your child has a credit report close to the child’s 16th birthday. If there is one – and it has errors due to fraud or misuse – you will have time to correct it before the child applies for a job, or a loan for tuition or a car, or needs to rent an apartment.
Protecting Our Children Online

(Click on link)

Protecting Our Kids Online
A cybersecurity expert talks about child safety online
http://news.yahoo.com/video/protection-kids-online-08000343.html
Whether playing, shopping, studying or just surfing, today's children are taking advantage of all that the web has to offer. But when it comes to their personal information, who's in charge? The Children's Online Privacy Protection Act, enforced by the Federal Trade Commission, requires commercial website operators to get parental consent before collecting any personal information from children under 13. COPPA allows teachers to act on behalf of a parent during school activities online, but does not require them to do so. That is, the law does not require teachers to make decisions about the collection of their students' personal information.

Many school districts are adopting Acceptable Use Policies (AUPs) to educate parents and students about Internet use and issues of online privacy and safety, and seek parental consent for their children's use of the Internet. For example, an AUP may tell parents about the privacy policies of online services with which a school has contracts and students' use of non-contract websites. It may include cautions against children disclosing personal information to websites - such as their full name, home or email address, and telephone number. Or it may tell parents that the school has established classroom email accounts rather than individual accounts if email communication is necessary between students and online services.

What is our school district’s policy about disclosing student information?

**Know Your COPPA Rights**
COPPA covers sites designed for children under 13 and general audience sites that know certain users are under 13. COPPA protects information that websites collect upfront and information that your children give out or post later.

**COPPA requires privacy policies.**
COPPA also requires these sites to post a privacy policy in a spot that's plain to see. The policy must provide details about what kind of information the site collects and what it might do with the information — for example, if it plans to use the information to target advertising to your children or to give the information to other companies. The policy also should state whether those other companies have agreed to keep the information safe and confidential.

**COPPA gives you the right to review collected information.**
As the parent, you have a right to see any personal information a site has collected about your child. If you ask to see the information, website operators will need to make sure you really are the parent; they may choose to delete the information. You also have the right to retract your consent, and have any information collected about your child deleted.
Check Out Sites Your Children Visit
If a site requires users to register, see what kind of information it asks for and determine your comfort level. You also can see whether the site appears to be following the most basic rules, like posting its privacy policy for parents clearly and conspicuously.

Review the privacy policy.
Just because a site has a privacy policy doesn't mean it keeps personal information private. The policy can help you figure out if you're comfortable with what information the site collects and how it plans to use or share it. If the policy says there are no limits to what it collects or who gets to see it, there are no limits.

Ask questions.
If you have questions about a site's practices or policies, ask. The privacy policy should include contact information for someone prepared to answer your questions.
Think Before You Share

What you post could have a bigger "audience" than you think.
Even if you use privacy settings, it's impossible to completely control who sees your social networking profile, pictures, videos, or texts. Before you click "send," think about how you will feel if your family, teachers, coaches, or neighbors find it.

Once you post information online, you can't take it back.
You may think that you've deleted information from a site — or that you will delete it later. Know that older versions may exist on other people's computers. That means your posts could live somewhere permanently.

Get someone's okay before you share photos or videos they're in.
Online photo albums are great for storing and sharing pictures of special events, and camera phones make it easy to capture every moment. Stop and think about your own privacy — and other people's — before you share photos and videos online. It can be embarrassing, unfair, and even unsafe to send or post photos and videos without getting permission from the people in them.
Mobile Sharing and Networking
Networking and sharing on-the-go can present unique opportunities and challenges. These tools can foster creativity and fun, but they could cause problems related to personal reputation and safety.

Use care when sharing photos and videos.
Most mobile phones now have camera and video capability, making it easy for teens to capture and share every moment. Encourage your teens to think about their privacy and that of others before they share photos and videos via cell phone. Get the okay of the photographer or the person in the shot before posting videos or photos. It could be embarrassing and even unsafe. It's easier to be smart upfront about what media they share at the outset than to do damage control later.

Use good judgment with mobile social networking.
Many social networking sites have a feature that allows users to check their profiles and post comments from their phones, allowing access from anywhere. Filters you've installed on your home computer won't limit what kids can do on a phone. If your teens are using a mobile phone, talk to them about using good sense when they're social networking from it.
Share with Care
(Click on link)

YouTube™:

Share with Care
What you post online could have an impact on people in the real world. To learn more about how your online actions can have real-world consequences visit
http://onguardonline.gov/articles/0033a-share-care
http://youtu.be/m_JB9mA_O3c
Heads Up: Stop. Think. Click
(Click on link)

YouTube™:

Heads Up: Stop. Think. Click
When you're online, take a second to stop and think before you click. To learn more about thinking before you click visit http://onguardonline.gov/articles/0033-heads
http://youtu.be/zdqVLeg6C9s
Cyberbullying is bullying or harassment that happens online. It can happen in an email, a text message, an online game, or comments on a social networking site. It might involve rumors or images posted on someone’s profile or passed around for others to see, or creating a group or page to make a person feel left out.

How do you respond to cyberbullying?

Help Prevent Cyberbullying

**Talk to your children about bullying.**
Tell your children that they can’t hide behind the words they type and the images they post. Bullying is a lose-lose situation. Hurtful messages not only make the target feel bad, but also make the sender look bad. Often they can bring scorn from peers and punishment from authorities.

Ask your children to let you know if an online message or image makes them feel threatened or hurt. If you fear for your child’s safety, contact the police.

Read the comments. Cyberbullying often involves mean-spirited comments. Check out your children’s page from time to time to see what you find.

**Recognize the signs of a cyberbully.**
Could your child be the bully? Look for signs of bullying behavior, such as creating mean images of another child. Keep in mind that you are a model for your children. Children learn from adults' gossip and other behavior.

Help stop cyberbullying.
Most children don’t bully, and there's no reason for anyone to put up with it. If your child sees cyberbullying happening to someone else, encourage him or her to try to stop it by telling the bully to stop and by not engaging or forwarding anything. Researchers say that bullying usually stops pretty quickly when peers intervene on behalf of the victim. One way to help stop bullying online is to report it to the site or network where you see it.

YouTube™:

Stand Up to Cyberbullying
You can help stop cyberbullies by standing up for yourself or someone else. To learn more about cyberbullying visit: http://onguardonline.gov/articles/0028-cyberbullying
http://youtu.be/lN2fuKPDzHA
What to do About a Cyberbully

**Don’t react to the bully.**
If your child is targeted by a cyberbully, keep a cool head. Remind your child that most people realize bullying is wrong. Tell your child not to respond in kind. Instead, encourage him or her to work with you to save the evidence and talk to you about it. If the bullying persists, share the record with school officials or local law enforcement.

**Protect your child’s profile.**
If your child finds a profile that was created or altered without his or her permission, contact the site to have it taken down.

**Block or delete the bully.**
If the bullying involves instant messaging or another online service that requires a "friend" or "buddy" list, delete the bully from the lists or block their user name or email address.

Cyberbullying Research Center
Facts About Cyberbullying Quiz
http://www.cyberbullying.us/quiz.php?QUIZNUM=1

STOP Cyberbullying: Are You a Cyberbully?
Take the quiz to find if you, too, are part of the cyberbullying problem!
http://www.stopcyberbullying.org/tweens/are_you_a_cyberbully.html
Children and Mobile Phones

Develop Cell Phone Rules:

• Explain what you expect
• Don’t stand for mobile bullying
• Set an example

Develop Cell Phone Rules

Explain what you expect.
Talk to your kids about when and where it's appropriate to use their cell phones. You also may want to establish rules for responsible use. Do you allow calls or texting at the dinner table? Do you have rules about cell phone use at night? Should they give you their cell phones while they're doing homework, or when they're supposed to be sleeping?

Don't stand for mobile bullying.
Children can use mobile phones to bully or harass others. Talk to your children about treating others the same way they want to be treated. The manners and ethics you've taught them apply on phones, too.

Set an example.
It's illegal to drive while texting or surfing or talking on the phone without a hands-free device in many states, but it's dangerous everywhere. Set an example for your children. Talk to them about the dangers and consequences of distracted driving.
Sexting: Don’t Do It

You may have heard stories at school or in the news about people "sexting" — sending nude photos from mobile phones. **Don't do it. Period.** People who create, forward, or even save sexually explicit photos, videos, or messages are putting their friendships and reputations at risk. Worse yet, they could be breaking the law.
This game will help the students understand how to protect themselves online. Each correct answer will reveal a tip on how to protect your information via Internet.

The Case of the Cyber Criminal - A techie spy and his cunning crew are out to get your personal information. Stop them cold by proving you’re ready to protect yourself online.
In Guided Practice, the students will make their own picture door organizer. During Independent Practice, the students will gather the information and pictures which will be included in the project. Remember, these are not scrapbooking projects. If students want to embellish their projects, they can take them home to work on them. Do not allow class time for this. This picture door organizer will be used to illustrate key points on keeping children safe when using technology and help students organize the information on hand.
References and Resources

Microsoft Clip Art: Used with permission from Microsoft

Websites:

Protecting Our Kids Online
A cybersecurity expert talks about child safety online

How to Protect Kids’ Privacy Online: A Guide for Teachers
Whether playing, shopping, studying or just surfing, today’s kids are taking advantage of all that the web has to offer. But when it comes to their personal information, who’s in charge?
http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec10.shtm

Net Cetera: Chatting with Kids About Being Online
This guide will help you offer the people in your community information about protecting kids online.

OnGuard Online: Protect Kids Online
Kids have lots of opportunities for socializing online, but they come with certain risks. Parents can help reduce these risks by talking to kids about making safe, responsible decisions.
http://www.onguardonline.gov/
References and Resources

YouTube™:

Heads Up: Stop. Think. Click
When you’re online, take a second to stop and think before you click. To learn more about thinking before you click visit http://onguardonline.gov/articles/0033-heads
http://youtu.be/zdqVLeg6C9s

Share with Care
What you post online could have an impact on people in the real world. To learn more about how your online actions can have real-world consequences visit
http://onguardonline.gov/articles/0033a-share-care
http://youtu.be/m_8Bmk4_03c

Stand Up to Cyberbullying
You can help stop cyberbullies by standing up for yourself or someone else. To learn more about cyberbullying visit: http://onguardonline.gov/articles/0028-cyberbullying
http://youtu.be/NI7fjuFPDHA