Teach good digital habits and know the risks

Team up with kids to explore cyberspace safely, using a mix of guidance and monitoring.

Seize the opportunity while your children are young to help them establish the good digital habits and skills they'll need to deal with situations, information, and people online. Then, as they demonstrate readiness, help them use new services and tools.

Start by educating yourself about the risks on the Internet. Not understanding how to use the Internet safely, young web surfers may:

> Reveal personal information that makes them vulnerable to bullies or exposes them to other risks, including those who pretend to be friends, but don't mean well.

> Stumble upon inappropriate material including hateful or sexual content by clicking a link in email, on a social network, or on the web.

> Click a flashy ad or open an enticing "free" game, which may download a virus, spyware, or other malicious software.

Others may unintentionally or deliberately expose children's information. Your child's school or club website may share too much personal information. Friends and family may expose children through comments and photos. Some sites share or sell—even own—the personal data they collect.

What to do if there are problems

Teach children to listen to and trust their instincts

If something feels uncomfortable or alarms them, that's a good warning sign. Let kids know they can come to you and that you will help solve the problem. Agree that you won't take away their phone or curtail privileges because of someone else's actions.

Immediately report

> Physical threats, persistent cyberbullying, or any form of exploitation to the police and the carrier. (Consider blocking the caller.)

> Inappropriate behavior to the school (if it involves another student) and to the phone carrier or web service. For example, in Microsoft services or software, look for the **Report Abuse** link, or contact us at **microsoft.com/reportabuse**.

More helpful info

> Learn how to create strong passwords: **aka.ms/passwords-create**.

> Find out how you can help protect your child's privacy: **onguardonline.gov/topics/kids-privacy.aspx**.

> For age-based guidance, visit **microsoft.com/security/family-safety/childsafety-age.aspx**.

> Get further child-oriented safety advice: **aka.ms/childsafety**.

Content contributor LOOK**BOTH**WAYS
ilookbothways.com

This material is provided for informational purposes only. Microsoft makes no warranties, express or implied.

1011 PN 098-110838

Microsoft

Protecting Young Children Online

> Teach good digital habits and know the risks

> Practical advice to keep young kids safer on the Internet

> What to do if there are problems

Microsoft

Practical advice to keep young kids safer on the Internet

Pay attention to what kids do and who they meet online

> Evaluate the devices and websites children want to use beforehand. Experiment to make sure you're comfortable with the functionality available such as GPS on mobile phones, computer webcams, and the ability to send unfiltered images or download applications (*apps*). Restrict any functionality your child isn't yet ready for.

> Sit with children while they play (or play together with them) so they can show you what they're doing and who they're interacting with.

> Put Internet-connected game consoles and computers in a central location. Consider using family safety technology that lets you monitor and review children's web activity.

> Watch for changes in behavior that may be signs of cyberbullying or other problems—for example, uncharacteristic reluctance to go online, unusual secretiveness, or spending too much time online.

Set clear rules

Before children begin using the Internet, discuss the kinds of sites that are off-limits, what information should not be shared, and boundaries for communicating respectfully. Explain that the rules are to protect, not control, them.

Teach kids to keep personal information private

Stress the value of personal information—passwords, age, phone numbers, full name, photos, home and email addresses, even feelings—to those who may want to exploit it. Show them how to:

> Choose an email address and online name that disclose nothing personal and aren't suggestive. Make sure real names aren't revealed when sending email. (Find out how: **aka.ms/hide-name**.)

> Ask before sharing personal information about themselves, friends, or family in texts, email, or on social sites.

> Create strong passwords. Don't share them with anyone but parents or a trusted adult—not even best friends.

Remind kids to respect others

> Be kind. Posting mean comments, cyberbullying, or cheating is not acceptable.

> Be honest. Stealing from other players in games, or downloading music, games, and other copyrighted material is illegal.

Teach kids safe and responsible computer use

They should:

> Not open attachments or click links with free offers in ads, contests, games, or email (even from friends).

> Be choosy about accepting new friends on phones and social sites or in games.

> Be skeptical. Not everything they see online is true, nor is everyone who they say they are.

> Say "NO" to and stop contact with anyone who wants to have a secret friendship. Don't respond to bullies.

Put technology to work

Use tools to keep kids safer

These can help you block harmful content and sharing of personal information, manage the sites children visit and their time online, monitor contacts, and watch for behavior like cyberbullying.

For example, Microsoft offers free safety features in its products: **aka.ms/compare-tools**.

Defend your computer against Internet threats

Start by keeping all software (including your web browser) current with automatic updating. Install legitimate antivirus and antispyware software. Never turn off your firewall, and use flash drives cautiously. Microsoft can help you: **microsoft.com/security/pypc.aspx**.

Protect your child on a mobile phone

> Lock it with a PIN to keep anyone from using it to call, text, or get personal info. Teach your child never to share the PIN.

> Consider disabling the location features on the camera of your child's phone.

Be the administrator of home computers

Learn to create different user accounts so you can manage your child's settings: **aka.ms/childsafety**.