CONNECT WITH CONFIDENCE:
Parent Guide for Digital Literacy
You don’t have to be a technical whiz to “BE a PRO” with technology!

With credible research from information security experts, public health professionals, law enforcement, digital literacy experts, and media psychologists, iKeepSafe has identified six simple concepts to help you keep your family safe and connected with digital devices.

The following pages provide specific information and simple activities so that everyone—young and old, digital expert and novice—can connect with confidence.

You’re encouraged to review this information with the important people in your life and have an open dialog about its contents.
Maintaining a healthy balance between work and play, online and offline activities

Kids spend more time engaged with media than they do in any activity other than sleeping. And who can blame them? [1] The online world is loaded with interesting and entertaining activities designed to capture and hold our attention.

While young people participate in a number of positive activities online, such as using the Internet for school work (85%) [2], and staying in touch with friends they rarely see in person (82%) [3], there are some downsides too. One of these downsides is spending too much time with technology.

According to studies conducted by the Kaiser Family Foundation and Sesame Workshop [4], 8-year-olds in the U.S. spend as many hours engaging with various screens as they do in school, and preschoolers are spending about four hours per day on media—far more than they devote to reading and outdoor play!

Research shows that young people look to adult role models to learn how to conduct their online lives [5], so it’s important for us to be mindful of our own time with digital media. Achieving a healthy balance between online and offline activities is a lifelong skill that we can all learn and practice together.

Tips

- The American Academy of Pediatrics (AAP) recommends:
  - No TV or screen use for the first two years.
  - Limiting screen time to two hours per day after two.
  - Making children’s bedrooms “electronic media free.”
- Keep family time “media free” by banning digital devices from the dinner table!
- Help your children select creative alternatives to digital media consumption.
- Charge phones each night in a central location where they can’t interrupt sleep.
- Don’t use smartphones as alarm clocks.
- Dr. Rolando Diaz, clinical psychologist in a private practice, recommends no screens the last hour before bed for improved rest, health, and reduced anxiety.

Activity

Keep a media log for one day. Have family members track how many minutes they use on all connected devices (computers, cellphones, TVs, games, tablets). Talk about what time they felt was valuable and where there was waste. Consider going media free for one day. Talk about what you learn.

Learn More

Balancing Real Life with Screen Time
How Too Much Time Online Might Affect ADHD
Too Much Time Online
Online Time v.s. Family Time
When Internet Use is Too High
Screen Time and Our Mental Health
Keeping a Balance with Real Life When Gaming Online
More About Online Gaming
CyberWise “Balance Learning Center”
HELPING KIDS UNDERSTAND THE CONSEQUENCES OF THE ETHICAL CHOICES THEY MAKE ONLINE

Should I share that unflattering photo of my friend on Facebook? Is it okay to download a song I don’t have rights to? Is this news or just gossip?

The online world constantly calls upon us to make ethical decisions like these.

While these questions are challenging for adults, just imagine how tricky they must be for young people who are still developing the cognitive skills required for ethical thinking. In fact, research from the Harvard School of Education’s GoodPlay Project indicates that most young people are devoid of ethical thinking or consideration for others when using the Web. [1]

In the past adults have played an important role in helping young people with ethical decisions. But when it comes to Internet spaces, kids got there first, and adults are largely absent from the online world where children and youth need ethical guides the most.

By talking together about issues like plagiarism, piracy, hacking, and more, we can help young people understand that a decision made today can have lifelong consequences.

Additionally, it’s critical to have regular discussions about the risk of taking, sending and/or viewing obscene content. Though 75% of US teens say sending sexually suggestive content “can have serious negative consequences,” 39% have sent or posted sexually suggestive emails or text messages [2]. In addition to the serious legal ramifications of “sexting,” there is compelling evidence that pornography has serious negative effects on children [3]. Medical research confirms that exposure to violent media is highly correlated with aggressive behavior. It is also illegal in every state to provide pornography to children.

Helping children and youth clearly understand the ethical expectations of their parents and society is a responsibility we all share.

TIPS

- Make sure your kids know your expectations for content they view and create, and don’t be afraid to set limits. Help them understand long term consequences of viewing violent or pornographic content.
- Use technology—filtering and monitoring software—to help you manage what comes into your house and when kids have access to it.
- Read and abide by the terms of use of each platform or site you visit.
- Avoid stealing of any kind.
- Respect other citizens, online and off.
- Accurately represent authorship.
- Always acknowledge when you use ideas taken from another source.

ACTIVITY

Create family guidelines for good sharing practices. Then browse through your own or your child’s social network accounts together. Look for activity that reinforces your family’s guidelines and point out how some posts don’t meet your expectations.

LEARN MORE

Texting Intervention Plan
Cheating and Technology
Downloading Music and Videos Legally
Helping Kids Understand the Consequences of Online Actions
Pornography Impacts Kids
Upstander Intervention
What is Really Meant When You Hear the Phrases Netiquette or Online Ethics?
How Do I Correctly Cite Internet Sources?
What Do I Do If I See Someone Else Harassed Online?
Getting and Giving Respect Online
CyberWise “Ethical Use Learning Center”
The American Library Association describes a digitally literate person as someone who “understands the relationship between technology, lifelong learning, personal privacy, and stewardship of information.” [1] Understanding what personal information is safe to share online—and what is not—is a critical aspect of modern life. According to experts at Reputation.com:

Sharing personally identifiable information such as home addresses, phone numbers, and excessive pictures should always be avoided. It is important to establish with your child at an early age the difference between personal information and public information.

As your child gets older, focus on reinforcing that message, but also explain the nuances between public and private sharing. By the time kids are in high school, they should be keeping most of their personal information private, but they should also consider using the Internet to share positive content about themselves to build a strong online reputation to attract college admissions officers and potential job recruiters later in life.

TIPS

Reputation.com recommends the following specific guidelines for each age group:

Elementary School Kids should NEVER share (their own or another’s):
- Age
- Full Name
- Address
- Phone Number
- Name of School
- Password Information
- Images (with possible exceptions depending on parental involvement, for example, sharing a child’s award on a family blog)

Middle School Kids should NEVER share (their own or another’s):
- Age
- Full Name
- Address
- Phone Number
- Name of School
- Password Information (even to friends)
- Most Images (at this age, kids get into social networking and will be sharing images via cell phones and digital cameras. Parents should focus on limiting the images their children share online)

High School Kids should NEVER share (their own or another’s):
- Address
- Phone Number
- Password Information (even to friends)
- Offensive or Sexually Suggestive Images or Messages

ACTIVITY

Sit down together and set up passwords on cell phones and tablets. Review the privacy settings on the social networking services used by your family.
All parents want their children to grow up having safe and healthy relationships. Today, young people maintain relationships on social media sites like Facebook, Instagram, Tumblr, and in online games... that is, when they’re not texting!

U.S. teens send an average of 3,364 mobile texts per month, more than doubling the rate of the next most active group [1]. Fully 95% of all young people ages 12-17 are now online and 80% of those online teens are users of social media sites [2]. Research shows that the majority of kids’ online relationships are with people they already know and in general, contrary to adult concerns, time spent online does not mean they are spending less face-to-face time with their friends. Social media, it turns out, actually facilitates (and strengthens!) offline interaction [3].

Although 70% percent of people worldwide say that the Internet has improved their relationships [5], occasionally unhealthy or even dangerous relationships can develop. In addition, research shows 90% of boys and 70% of girls aged 13 to 14 have accessed sexually-explicit content at least once [6]. Compelling evidence confirms that exposure to pornography will affect youths’ ability to form and maintain healthy relationships. [7]

Surprisingly, when researchers from Pew Internet asked teens, “Who has been the biggest influence on what you think is appropriate or inappropriate when you are using a mobile phone or going online?,” 58% of respondents said their parents, with “friends” following with only 18% [5].

This is good news for parents! Why not take a step through this open door and talk to your family about maintaining safe and healthy online and offline relationships. iKeepSafe offers some terrific tips to get this conversation started.

TIPS

Ask your children:

🌟 How might these technologies hurt your relationships?
🌟 Have you ever felt pestered or overwhelmed by digital communication from a friend or boy/girlfriend?
🌟 Some students are pressured to send a sexually explicit text or photo. Has this happened to you? How can we handle these uncomfortable situations to prevent them from happening?

ACTIVITY

Sit down together and review the Friends List on the social networking sites that you and your child use. Delete people you don’t really know.

LEARN MORE

Understand the Community’s Roles
Cyberbullying
Cyberbullying: How Young Does It Start?
Students Post Inappropriate Rankings Online
Digital Dating Abuse Is a Pervasive Problem
Facebook Grieving—How Social Media Helped Us Say Goodbye
Learning in Times of Facebook Trauma
What Is So Wrong with Sexting?
How Many Online Friends Do You Have?
The Positive Power of Online Collaboration
Connecting Grandparents and Grandkids through Technology
How to Help Kids Deal with Betrayal Online
CyberWise “Relationships Learning Center”
BUILDING A POSITIVE ONLINE REPUTATION THAT WILL CONTRIBUTE TO FUTURE SUCCESS

Everything we post online—and everything that others post about us—contributes to our permanent, digital reputation.

While this is good news when the information is positive, it can be disastrous if negative or inappropriate comments or photos find their way online, because there is no erase button on the Internet!

It is important to help kids understand that everything online is persistent, searchable, replicable, and can be viewed by vast invisible audiences [1]. In other words... that photo they posted of themselves partying with a lampshade on their head? . . . it stays in the digital stratosphere forever, can be searched for and found by anyone and everyone. It can be copied, reposted, shared, and viewed by strangers around the world. Ouch! That can hurt when applying for college or a job.

On the other hand, creative projects, awards, and documentation of service experiences can be an inspiration to other students and go a long way in setting yourself apart from other applicants.

While young people can’t be expected to fully understand the enormity of these consequences (who can for that matter?), it is important for families to talk about how to manage their online reputations and to agree on family guidelines.

TIPS

🔹 Think before you share.
🔹 Encourage your child to post positive items and accomplishments online for college recruiters and future employers.
🔹 Have your child consider replacing an immature or inappropriate email address with something more serious.
🔹 Sit with your child and review posts on their own and on their friends’ social networks. Discuss which images and posts might help their online reputation and which ones might hurt.

ACTIVITY

Have each family member do an Internet search of their own name to see if they already have a digital footprint and learn what it says about them. Also do a separate image and video search. Discuss what you find.

LEARN MORE

Re-thinking Blog and Blog Venting—Consider Your Future Digital/Online Reputation Social Networks and Positive Online Reputation Information is Permanent What Should My Kids Understand before Posting or Viewing Videos on YouTube? What to Do if My Child Has an Inappropriate Video on YouTube? Hey Teens, Chances Are You’ll Regret Oversharing Personal Information Online CyberWise “Reputation Learning Center”
OBSERVING GOOD HABITS FOR SECURING HARDWARE AND SOFTWARE

With all the exciting things the digital world has to offer, it’s easy to overlook simple strategies that can keep us safe online.

Research shows that in terms of online security, most people fall short [1]. As a result, one in six Americans will be the victim of identity theft [2].

This may sound daunting, but by following a few simple strategies, even adults with limited technical skills can help their families be safe and secure online. As the primary gatekeepers and managers of children's Internet experience [3], it’s our responsibility as parents to protect sensitive data, maintain secure networks, and to filter and monitor access shared by our children.

Start by having a conversation with your entire family about choosing secure passwords and keeping them in a safe place. Learn how to back up your data and how to install anti-virus software. Adjust the privacy settings on the search engines and the social networking sites you use, and gain a general understanding of the hardware, software, and social platforms your family members visit the most. By reviewing the following guidelines you’ll be well on the road to achieving online security.

**LEARN MORE**

- Avoiding Internet Crooks at Tax Time
- New Recourse for Protecting Kids from Cyber Impersonation
- Password Safety and Security
- Blog Safety
- Securing Your Wireless Internet
- How Can I Avoid Spam and Phishing Scams?
- What Can I Do to Help My Family Be Safer Online?
- Safe and Secure Online Banking
- CyberWise “Online Security Learning Center”

**TIPS**

- Back up your data.
- Keep all of your software current with automatic updating. These updates can help prevent personal information from being stolen.
- Install antivirus and malware protection.
- Protect your wireless network by using a network key (password), and set the password on your router, so router settings can’t be changed without your knowledge.
- Use long passwords that contain a combination of letters, numbers, and symbols.
- Use different passwords for different sites and mobile devices. Never use your email username and password for social media or other logins.
- Look for “settings” or “options” on social networking sites use to manage the personal information you share.
- Use passwords on all networks and personal devices that connect to your network. One weak link can leave all your devices vulnerable.
- Monitor and track all devices used by minors—cell phones, computers, game consoles, etc. Monitoring software and parental controls offered by your cell phone provider or other third party providers will help you monitor and direct when and where your kids go online and use their cell phones.
- Teach your children how and when to report stalking, harassment, inappropriate photos, and threats; all of these are prohibited on social media sites (like Facebook and Twitter), and often are punishable by law.

**ACTIVITY**

Sit down together and test the strength of your passwords at [www.passwordmeter.com](http://www.passwordmeter.com). Do the iKeepSafe Password Activity (page 2).
Citations

BALANCE


ETHICAL USE


PRIVACY

2. Reputation.com, and private email communication with iKeepSafe.

REPUTATION

2. Reputation.com

RELATIONSHIPS

2. Lenhart, A., et. al., “Teens, kindness and cruelty on social network sites” (Nov. 9, 2011), Pew Internet.

3. Jepson, J., “Study: Online social networking leads to more personal interaction” (October 29, 2010). KSL.


ONLINE SECURITY
