Internet Safety

https://www.commonsense.org/education/digital-citizenship/internet-safety

Internet safety or "e safety" has become a fundamental topic in our digital world and includes knowing about one's Internet privacy and how one's behaviors can support a healthy interaction with the use of the Internet. Students explore how the Internet offers an amazing way to collaborate with others worldwide, while staying safe through employing strategies such as distinguishing between inappropriate contact and positive connections. These foundational skills and learning more about the Internet safety definition helps students learn how to be safe on the Internet.

The term "online predator" often conjures up the image of a creepy older man at a computer screen waiting to lure an unsuspecting child. The media reinforces this depiction, which is problematic because it does not fit with the kinds of risky relationships that are more common for kids and teens or necessarily follow Internet safety statistics. In reality, when online sexual solicitation does occur, it's more likely to be between two teens, or between a teen and a young adult. The following information serves to clear up these misconceptions and helps to showcase some of the Internet safety facts by providing information for teachers about the myths and realities of online sexual solicitation, as well as guidance on how to approach this sensitive topic.

Thinking Beyond "Online Predators" & How to be Safe on the Internet

1. Teens, not children, are most likely to receive online sexual solicitations. Online solicitors rarely target younger kids. This happens more frequently to younger teens (ages 14 to 17). People who solicit online are often upfront about their intentions. They may ask teens to talk about sex, to give out personal sexual information, to send sexy photos online, or to meet offline for a possible sexual encounter.
2. A teen is more likely to be solicited online by another teen or a young adult. Contrary to popular belief, teens are more likely to be solicited online by similarly aged peers. It is true, however, that a very high majority of sexual solicitations online come from boys or men. Guiding teens to think more generally about avoiding risky online relationships, rather than telling them to fear predators, prepares them for the wider breadth of situations they may have to deal with online—not only the extreme cases.
3. The "predator-prey" label gives the wrong impression. There is a range of behaviors that are not made clear by the predator-prey label. The behaviors can range from "not as risky" (i.e. receive inappropriate spam through email and immediately send to their junk mail) to "very risky," (i.e. seek companionship or friendship on an online chat room, and develop an ongoing, risky relationship with a stranger).

In the most extreme cases of online solicitation – those involving older adults and teens – targets are usually aware of their solicitor's true age and intentions. For the small percentage of teens who find themselves in this kind of situation, simply warning them against "unwanted contact" is not an effective strategy because they have likely grown to be comfortable with, and perhaps even dependent upon, their solicitor. Instead, we need to help teens understand why it is risky to flirt with people they meet online, how to recognize warning signs, and more broadly, why romantic relationships between teens and adults are unhealthy.

The Truth About Risky Online Relationships

Many adults fear that kids use the Internet to connect with strangers. In reality, most kids and teens use the Internet to keep in touch with people they already know offline, or to explore topics that interest them. Studies show that it is most often teens who are psychologically or socially vulnerable that tend to take more risks online (Subrahmanyam and Šmahel, 2011; Ybarra et al., 2007). These at-risk teens might seek reassurance, friendship, or acceptance through relationships that they develop online — in chat rooms, online forums, etc. The term "grooming" is sometimes used to describe the process of an older adult coaxing a young person into sexual situations. For cases involving children, grooming may involve befriending the child, showing interest in his or her hobbies, exposing the child to sexually explicit material, and manipulating a child into a sexual encounter (Lanning, 2010). The term is less commonly used for cases between teens, or between a teen and a young adult. Research also shows that teens who flirt and engage in online sexual talk with strangers– especially in chat rooms – are more likely to be solicited for sex (Ybarra et al., 2007).

What Should Kids and Teens Know if Online Strangers Contact Them?

Elementary School:

Discuss with kids what it's like to have a "gut feeling" about an uncomfortable situation. You can use a traffic light analogy (green = okay, yellow = iffy, red = risky) to help kids assess different online scenarios (e.g., if someone asks for a photo, talks about inappropriate things, asks them to keep anything a secret, bothers them, says something that makes them them feel sad or upset). You might be tempted to lean on typical "stranger danger" messaging here, but do consider that these situations may also happen with people kids know or sort of know. Emphasize to students that they have the power to end conversations and log off the Internet at any time, and to not let shyness or embarrassment prevent them from talking to a parent or family member if they get into an iffy or risky situation. This approach can apply beyond grooming to issues like cyberbullying and online scams, too.

Middle School and High School:

We recommend avoiding fear-based messages with teens, as research indicates that teens are less responsive to this approach (Lanning, 2010). Teens are not likely to buy into the idea that they should avoid all contact with anyone they do not know online. After all, it is nearly impossible to connect with others online without talking to some people who are strangers. Rather than telling teens to never talk with strangers, it is more effective to have conversations about why certain online relationships are risky, and about how to avoid them. The number one thing for teens to remember is that they should avoid flirting with or regularly talking to online strangers or online acquaintances, especially – but not only – if the person they are chatting with is older than they are. Teens should also reflect on these questions if they communicate with someone they meet online:

- Has this person asked to keep anything about our relationship a secret?
- Has this person hinted at or asked about anything sexual?
- Have I felt pressured or manipulated by this person?
- Do I feel true to myself – sticking to my values – when I communicate with this person?

Privacy & Security

Just as in real life, it's important for young people to know whom they can trust with their information online. Though security programs and privacy settings can help block some issues, such as computer viruses and cookies, kids should also learn how to create strong passwords and protect their private information. Starting in elementary school, kids can learn the importance of looking at a website's privacy policy with their families and asking for permission before creating accounts or downloading files. Older teens can learn concrete strategies for identifying scams, as well as limit the types of information that companies collect about them through apps and websites. Developing skills around Internet privacy and safety can help set a strong foundation for students and their digital lives.

The Dos and Don'ts of Creating Strong Passwords

- Do make your passwords eight or more characters, using combinations of letters, numbers, and symbols. (These are harder to crack than regular words because there are more combinations to try.)

- Don't include any private-identity information in your password. (People may easily guess passwords that include your name, address, birth date, and so on.)
- Do change your password at least every six months. (This way, even if someone does guess your password, they won't be able to get into your account for long.)
- Don't share your password with your friends. (Even if you trust them, they might unintentionally do something that puts you or your information at risk.)

Why Teach It

Help your students …

- identify strategies for creating and protecting strong passwords;
- spot and avoid online scams;
- and understand the concept of Internet safety and privacy, why companies collect information, and how to understand privacy policies.

Kids may not realize they're putting their information in jeopardy, because the warning signs aren't always obvious. With your help, students can master the fine art of password creation, recognize and avoid online scams, and distinguish positive and safe sharing from oversharing. These skills are crucial to the security of the digital devices your students use as well as the information those devices store. Otherwise, your students may expose themselves and their families to serious issues, such as computer viruses or data and identity theft.

Relationships & Communication

Whether we're reading an online review, posting something on a social-networking site, texting a friend, or sharing a photo through an app, we're participating in a world where we can be instantly connected to thousands of people at a moment's notice. When kids connect with each other from a distance or through a screen name, it can affect the way they behave. For example, their actions can feel removed from consequences or free from discovery. When people are anonymous, it's easier to behave irresponsibly, cruelly, or unethically. Others may simply misinterpret the tone and context of messages or posts. Kids need a code of conduct for using the Internet and mobile media just as they need a code of conduct in the offline world. They should be empowered to be good digital citizens, in addition to being good citizens in general.

Why Teach It?

Help your students …

- recognize that different audiences require different types of communication and online etiquette;
- develop constructive solutions to online interpersonal dilemmas that exemplify ethical behavior;
- and imagine the motivations, feelings, and intentions of others as they relate to a variety of online exchanges.

Anything your students say or do with their phones or through quick messages may seem to disappear when the devices shut down, but the impact on others remains -- whether good or bad. As a teacher, you can guide your students to think critically about different forms and norms of digital communication. Guide them to choose their words wisely. Help them develop the habit of self-reflecting before posting or texting, asking themselves questions such as "Who is my audience?" and "What's the purpose of this message?" and "In what context will people be reading this?" With your help, they can learn to recognize that their decisions online can have more far-reaching benefits and consequences than their actions offline because of technology's power to connect.

Cyberbullying & Digital Drama

It seems like there are new cyberbullying stories (also known as “cyber bullying" or “cyber–bullying”) in the headlines each day. The effects of cyberbullying can be devastating for everyone involved. Cyberbullying statistics have shown that modern technology with its ability to increase our connectivity can also be the perfect platform for bullying.

Students can learn what to do if they are involved in a cyberbullying situation as well as ways of how to stop cyberbullying by exploring the roles people play and how individual actions — both negative and positive — can impact their friends and broader communities. Students are encouraged to take the active role of upstander and build positive, supportive online communities.

What to Know

It’s time to know the cyberbullying facts. Online cruelty, also referred to as cyberbullying, takes place whenever someone uses digital media tools such as the Internet and cell phones to deliberately upset or harass someone else, often repeatedly. While spreading rumors and bullying is nothing new for kids, online tools can magnify the hurt, humiliation, and social drama in a very public way.

Cyberbullying can take a variety rumors, or posting cruel comments or images online. The feeling of being anonymous or “removed” from a target in an online environment can encourage a kid who normally wouldn’t say anything mean face-to-face to act irresponsibly or unethically. With the effects of cyberbullying ranging from low self-esteem to depression to thoughts of violence or suicide, it is important for parents, teachers and students alike to learn how to prevent cyberbullying and stop it in its tracks.

Why Teach It

Help your students…

- consider ways to create positive online communities rooted in trust and respect.
- learn to identify, respond to, and limit the negative impact of cyberbullying and other unethical or harmful online behaviors.
- recognize their own role in escalating or de-escalating online cruelty as upstanders, rather than bystanders.

When kids misuse online or mobile technology to harass, embarrass, or bully others, they can do real and lasting harm. Nothing crushes kids' self-confidence faster than humiliation. And just imagine a public humiliation sent instantly to everyone they know. Sadly, hurtful information posted on the Internet is extremely difficult to prevent or remove, and millions of people can see it. As more and more states take a harsher stand with new cyberbullying laws, it is important to know how to stop cyber bullying in its tracks. Teachers and parents can help kids think about the consequences of their online actions — before they even occur. When guiding students, it's important for them to understand that they have a choice in all of their online relationships. They can say something positive or say something mean. They can create great community support around activities or interests, or they can misuse the public nature of online communities to tear others down.

Key Vocabulary

Cyber bullying: the use of digital media tools such as the Internet and cell phones to deliberately upset or harass someone.

drama: the everyday tiffs and disputes that occur between friends or acquaintances online or via text. Note: Unlike cyberbullying, which involves repeated digital harassment toward someone, drama is broader and more nuanced. That being said, kids and teens sometimes use the term drama to distance themselves from emotionally difficult behavior. Digital drama can still feel very real to students, lead to hurt feelings, and even damage friendships. In some cases, digital drama can escalate into an offline fight – either verbal or physical.

hate speech: making cruel, hostile, or negative statements about someone based on their race, religion, national origin, ability, age, gender, or sexual orientation.

target: a person who is the object of an intentional action.

offender: a person who has a malicious intent to hurt or damage someone.

bystander: a person who does nothing when they witness something happening.

upstander: a person who supports and stands up for someone else.

escalate: to increase or make more intense.

de-escalate: to decrease or make less intense.

Digital Footprint & Reputation

What is a digital footprint and why is it important to know about it?

Students learn to protect their own privacy and respect others' privacy. Our digital world is permanent, and with each post, students are building a digital footprint. By encouraging students to self-reflect before they self-reveal, they will consider how what they share online can impact themselves and others. Awareness about one's own digital footprint can also help to support digital literacy.

What to Know

In a world where anything created online can be copied, pasted, and sent to thousands of people in a heartbeat, privacy starts to mean something different than simply guarding personal information. On the positive side, this culture of sharing holds tremendous promise for young people to express themselves, collaborate, and find support for their ideas and interests. However, the ease of online disclosure also poses risks for young people. A decision made in the spur of a moment — a funny picture, a certain post — can resurface years later. Something originally sent to a friend can be sent to a friend's friend, and so on. That's how secrets become headlines and how false information spreads fast and furiously – to classmates, teachers, college admissions officers, future employers, or the public at large.

Why Teach It

Help your students …

- become aware of the “digital footprint” they leave online and reflect on the kind of personal information to share about themselves, depending on the content, context, and audience.
- celebrate a “culture of sharing” through digital media while considering some possible harmful effects of over-sharing and Internet privacy.
- learn to respect the privacy of others online when tagging, posting, or copying other’ personal information.

By guiding your students to self-reflect before they self-reveal, you can help them learn to consciously manage their own privacy online, as well as respect the privacy of others. If students aren’t careful about what, how, and to whom they disclose information online, it may be used or interpreted in ways they never intended. Help them understand the public and permanent nature of the Internet so they can begin to build a positive digital presence.

Self Image & Identity

Whether designing avatars for virtual worlds, selecting profile pictures, or carefully crafting texts to friends, young people have countless opportunities to express themselves through digital media. On the one hand, playing around with creative identities can be a safe and imaginative way for kids to explore who they are. Having a different persona online can also be a real gift for a kid who's particularly shy. On the other hand, a digital identity can be a way for kids to dodge personal consequences. When kids are disguised or anonymous, they can push limits and act in ways they wouldn't in the real world. Some may explore antisocial or harmful identities. Others simply overshare and create reputations that might come back to haunt them. Either way, if there's a large gap between an online and an offline identity, it can fragment a kid's sense of self (especially when the online identity gets a lot of feedback and the kid becomes dependent on it).

Why Teach It

Help your students...

- understand the similarities and differences in how they present themselves online and offline;
- reflect on how the Internet allows for anonymity and deception and explore how this can affect their behavior online;
- and consider the motivations, benefits, or possible harm to oneself and others when assuming an online identity that's different from one's real self.

Help your students consider how their identities -- online and offline -- may affect their relationships, sense of self, and reputation. Give them opportunities to teach you about the websites and apps they use most, as well as describe any unspoken rules about communication in these spaces. By setting the tone for an open dialog, you can then steer discussions to address the benefits and risks of online self-expression. Talk to them about anonymity and why it's important to be responsible for their actions even when they aren't easily identifiable. Work with students' families to help communicate to them why identities grounded in hatred, violence, illegal activities, or risky sexual behavior should be avoided entirely. With this whole-community approach, students can learn to habitually reflect on how they can present themselves online in positive and beneficial ways.

Information Literacy

What is Information Literacy? Information literacy includes the ability to identify, find, evaluate, and use information effectively. From effective search strategies to evaluation techniques, students learn how to evaluate the quality, credibility, and validity of websites, and give proper credit. Information Literacy has also been referred to as digital literacy or media literacy. Regardless of the terminology, be it digital literacy or media literacy, having information literacy skills are the fundamentals to thrive in a digital space.

What to Know

Today’s digital landscape offers young people unprecedented access to tools and resources for learning. The information that kids encounter, however, is not always accurate or high-quality. Foundational information and digital literacy skills, such as conducting strategic online searches, judging the legitimacy of online sources, sifting out misinformation, and recognizing advertising, can help set kids up for success as lifelong learners. For example, kids can learn to search effectively and efficiently with the right kinds of keywords. They also can learn that sponsored links (which commonly appear at the top of the search result list) are forms of ads and therefore not always the best resources. When young people also get in the habit of checking out an author’s credibility or bias, questioning whether a photo has been digitally altered, or cross-referencing sources, they can avoid being misinformed or duped.

Why Teach It

Help your students …

- learn effective techniques for evaluating the quality and credibility of websites.
- think critically about the intentions of commercial websites and advertising.

- apply different search strategies to increase the accuracy and relevance of online search results.

Too often, students who are looking for information online— particularly for their schoolwork — conduct an oversimplified search that leads to millions of results. With a sea of information at their fingertips, it is crucial for young people to think about how they search and what they find online. As a teacher, you can help your students develop strategies for uncovering accurate, relevant, and quality information — whether conducting online research for school projects or exploring their personal interests.

Key Vocabulary

strategy: a course of action designed to help you reach a specific goal or result

keywords: the words you use to search for information about a topic

plagiarism: using some or all of somebody's work or idea and saying that you created it

citation: a formal note of credit to an author that includes their name, date published, and where you found the information

digital photo manipulation: using digital technology to change the content or appearance of a photo

retouching: to improve a photo by adding or changing small details

synergy: two or more things working together to produce something that each could not achieve separately

collective intelligence: knowledge collected from many people toward a common goal

advertisement: a message that draws attention to a product and encourages people to buy it

banner ad: an online ad that looks like a bar or button on the website

advergame: an online ad that is also a game you can play video ad: an online ad that is a video and might look like a TV commercial

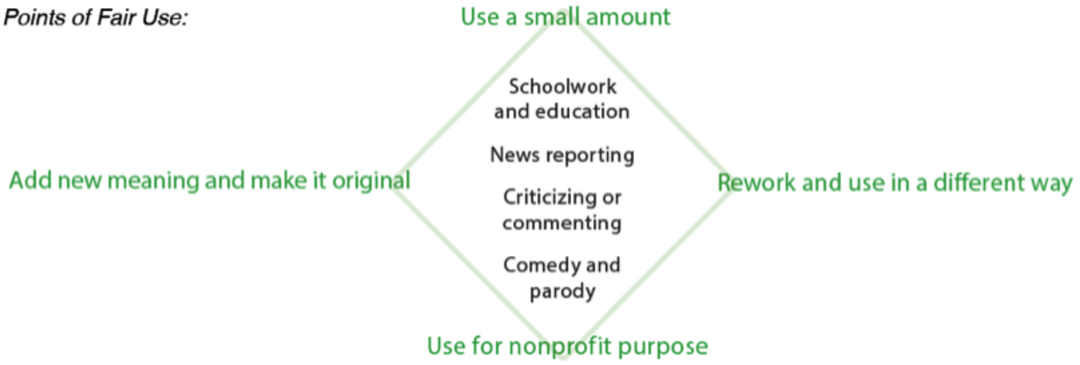
pop-up ad: an online ad that “pops up” over the content of the website sponsorship

ad: an ad that specifically supports an event, activity, person, or organization

Creative Credit & Copyright

We live in a digital culture that empowers young people to access information instantly, rework media easily, and share their creations globally. But the ease with which young people can find, copy, and distribute digital content can also lead them to use online material without thinking about where it comes from or to whom it belongs. Viewing the Internet as a "free-for-all" leads to problems of copyright infringement, plagiarism, piracy, and a general lack of respect for the hard work and creativity of others. The basic fact is this: Even if something is posted on the Internet for all the world to see, someone somewhere created that picture, song, or article -- and it belongs to that person.

The Four Points of Fair Use:


Use a small amount
Schoolwork and education
News reporting
Criticizing or commenting
Comedy and parody
Add new meaning and make it original
Rework and use in a different way
Use for nonprofit purpose

Why Teach It

Help your students …

- learn about their rights to their own copyrighted work;
- identify how they can use copyrighted work without permission through public domain and fair use;
- and understand that piracy and plagiarism are forms of copyright infringement that are unethical and unlawful.

By focusing on young people's roles as digital creators, you can encourage your students to take responsibility for positively shaping the creative online culture of which they are a part. They may not realize that copying and pasting material they find online into schoolwork without citing it is plagiarism. They may not understand that illegally downloading and sharing music, videos, and software is a form of stealing called piracy. With your guidance, your students can learn to respect the copyrights of others, as well as how to protect, receive acknowledgement for, and share their own original creations.