Microsoft

Free resources for teaching online safety

General information

- Get advice to help you teach good digital citizenship, as well as tools to help your school prevent, detect, and respond to cyber incidents: **generationsafe.ikeepsafe.org**.
- Use these classroom resources and materials to teach kids how to be more secure, safe, and ethical in their digital world: **staysafeonline.org**.
- Educators, parents, and kids of all ages can find online safety information written just for them: **netsmartz.org**.
- For your school, find out about email, programs like Word and Excel, and online storage from Microsoft—all free: **microsoft.com/liveatedu/free-email-accounts.aspx**.
- Special offers, free services, and more from Microsoft will help you get ready to go back to school: **microsoft.com/education**.

Curriculum and lessons

- NetSkills4Life offers a K-12 Internet safety curriculum (with about three hours of instruction per grade) to empower students to develop the skills and ethics to stay safer online: **netskills4life.com/teachers.html**.
- iKeepSafeAnyWhere.org hosts Internet security, safety, and digital citizenship lessons. Inspired by current events, the topics change frequently: **ikeepsafeanywhere.org/for-educators**.
- Videos about online safety, including gaming and cyberbullying: **nsteens.org/teachingmaterials**.

For tweens and teens

- An online forum where teens can chat with other teens (or become cyber mentors): **cybermentors.org.uk**.
- Direct talk about what it really takes to be both safe and savvy online: **tinyurl.com/iLBW-teen-safety**.

Content contributor

iKeepSafe
Generation Safe
New Media Mentor for Digital Citizenship with 360 Self Assessment Tool

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

1011 PN 098-117542

Top Tips for Online Safety in Secondary Schools

Youth today spend half of their waking hours using technology, which helps to define and shape their identities and relationships, and directly impacts the school environment. We have a responsibility to understand online safety for ourselves, and then help guide kids to be safer in this connected world.

Good digital practices for educators

The advice below comes from legal professionals working with educators. Acquaint yourself with school rules, and aim to keep your online personal and professional lives separate.

Understand school rules

- Post your school's Acceptable or Responsible Use Policy for technology and online access. Refer to it often, explaining it to your students as you apply it.
- Know your schools' plan for responding to cyberbullying, cyberstalking, hacking, sexting, plagiarism, and other potentially illegal online activities.
- Understand your school district's policy for teacher use of social media and interactions with students on social networks.

Communicate cautiously with students on social media

Your online exchanges with students aren't private. They can be inspected, taken out of context, or forwarded. Plus, after posting, they can be difficult to remove.

- Set boundaries when communicating online with students. For instance, avoid late-night exchanges, and don't discuss intimate topics such as dating.
- Protect the privacy of your students. Don't post anything about individuals on your social media pages.
- Use privacy settings to limit your exposure to students on social networks such as Twitter, Facebook, and photo- and video-sharing sites. This means not sharing with "friends of friends" in case some of your friends are connected with your students.
- Don't friend students on your personal sites or allow them to follow your personal Twitter feed.

Social networking safety

Learn more about how to protect your privacy on social networks and navigate them more safely: **aka.ms/socializing-online**.

Microsoft

Tips for teaching students online safety

As educators, you can help students become ethical, responsible, and resilient digital citizens. You don't have to be tech savvy: use the tips below that rely on common sense and basic computer safety practices. (To print a version of these tips that you can distribute to your students, visit **aka.ms/student-tips**.)

1 Protect your devices and info

Take these steps to guard Internet-connected devices against someone who tries to break in and impersonate or spy on you, scam you, or use malicious software to destroy or steal your photos, games, contact lists, and other info.

- Keep all software (including your web browser) current with automatic updating. Install legitimate antivirus and antispyware software. Never turn off your firewall. Protect your wireless router with a password, and use flash drives cautiously. Microsoft can help you do this: **microsoft.com/security/pypc.aspx**.
- Think twice (even if you know the sender) before you open attachments or click links in email or IM, or on a social site.
- Use strong passwords, and DO NOT SHARE THEM—not even with your best friend. Learn how: **aka.ms/passwords-create.**
- Lock your phone with a PIN to keep anyone from making calls, texting, or accessing your personal info.

2 Share with care

Information you share online about yourself or comments you post can become public. Plus, they may remain in search results for years to come, potentially visible to a future employer or college admissions officer.

Follow this advice to guard against someone turning your information against you to bully or impersonate you, steal your identity, or scam you.

- Don't share suggestive photos or videos. You lose control of where they go.
- Make your social network pages private. One way is to look for **Settings** or **Options** on the social site to manage who can see your profile or photos tagged with your name, how people can search for you, who can make comments, and how to block people.
- Create profile pages and email addresses that reveal nothing personal and aren't suggestive.
- Be choosy about adding new friends on phones or social sites, or in games.

3 Be a real friend

- If you wouldn't wear it (say, on a T-shirt), don't share it.
- Stand up for your friends. Cyberbullies are less likely to target someone who has a strong group of friends, and usually stop when a victim's friends rally around him or her. (Cyberbullies may be surprised to learn that their actions may be crimes.)
- Don't share online personal details of friends and family members without their permission.

4 Connect honestly and carefully

- Don't download copyrighted music, video games, etc.—it's illegal. Plus, pirated files are often used to distribute viruses and spyware without the user's knowledge.
- Don't be a Net cheater. Don't copy text from the web or buy finished essays or reports.
- Use only social networks that are right for your age, so you'll benefit from their age-based privacy protections.
- Meeting an online "friend" in person can be risky. Protect yourself: always bring a parent, trusted adult, or friend and meet in a busy public place.

Advice for parents

Parents experience daily the constant connection their kids have with technology and how it shapes their reality. That's why parents can play a vital role in helping their kids develop the skills and ethics they need to make their own informed decisions.

In your conversations with parents about online issues, suggest that they pay attention to what kids do and who they meet online. It's particularly important for parents to negotiate clear guidelines for web and online game use that fit both their kid's maturity and the family's values.

Refer them to this Microsoft brochure, written specifically for parents to help protect tweens and teens online: **aka.ms/tween-teen-safety.**