# Privacy Tips for Teens

## What you post lasts a lifetime

Share the best of yourself online. Before posting online, think about what others might learn about you and who might see it in the future – teachers, parents, colleges and potential employers.

## Be aware of what's being shared

Be aware that when you post a picture or video online, you may also be sharing information about others or personal details about yourself like where you live, your phone number, email address, or where you go to school.

## Post about others with permission

Post only about others as you would like to have them post about you. Ask permission before you tag a friend in a photo.

## Own your online presence

Limit who can see your information and what you share. Learn about and use privacy and security settings on your favorite online games, apps and platforms.

## Understand data collection

Know what's being collected, who is collecting it and how it will be used. Information about you, including the games you play, what you search for online and where you shop and live, has value. Be thoughtful about who gets that information and how it's collected through apps and websites. Think twice before you use apps that want access to use personal information (like your location or your contacts list) it doesn't need.

## Secure your devices

Protect your information if your device is lost or stolen by using strong passwords, passcodes or touch ID features to lock your devices. Avoid sharing your devices with others. Never share social media user-ids and passwords with others.

## Wi-Fi hotspots are not so hot

Public wireless networks and hotspots are not secure. Anyone can potentially see what you are doing on your laptop or smartphone while you are connected to these networks. Hackers position themselves between you and the connection point, so instead of talking directly with the hotspot, you're sending your information to the hacker. Limit what you do on public Wi-Fi, and avoid logging in on key accounts like email and financial services. Avoid using open Wi-Fi hotspots.

## Now you see me, now you don't

Disable Wi-Fi and Bluetooth when not in use. People are able to track you if your Wi-Fi or Bluetooth is turned on and while you are within range.