Keeping Our Children Safe Online

Technology is changing so fast that it is hard for us all to keep up with it. Primary age children who have grown up with it are comfortable using it in a way that parents sometimes aren't. Whilst in many ways our lives have changed for the better with these technological advances, we all need to be aware of the increasing risks and dangers our children face when using the internet, messaging systems, social networking and apps.

Please take some time to read this leaflet and to talk to your child about staying safe.

Spotlight on Age: Guidelines

Under 5's Checklist

START setting boundaries now – it's never too early to do things like set limits for the amount of time they can spend on the computer

KEEP devices like your mobile out of reach & make sure you have passwords/PINs set up for the times you might lend them to your child

CHECK age ratings on apps, games, TV & films before streaming or downloading

EXPLAIN your technology rules to grandparents, babysitters, etc so that they stick to them when they're looking after your child

SET the homepage of the family computer or tablet to an appropriate website like Cbeebies

Spotlight on Age: Guidelines

6-9's Checklist

CREATE a user account for your child on the family computer with appropriate settings & make the most of Parental Controls & tools like Google Safe Search

AGREE a list of websites they're allowed to visit & the kind of personal information they shouldn't reveal about themselves online (like the name of their school or their address)

DECIDE time limits for things like using the internet & playing on games consoles

BEAR in mind what older siblings might be showing them on the internet, mobiles, games consoles & other devices & agree some rules as a family

TALK to other parents about their views & don't be pressured by your child into letting them use new technologies

Spotlight on Age: Guidelines

10-12's Checklist

MAKE sure you've set some tech boundaries before they get their first mobile or games console – once they have it in their hands it can be more difficult to change the settings

REMIND your child to keep phones, etc well hidden to minimise the risk of theft

TALK to them about what they post & share online – written comments, photos & videos form part of their digital 'footprint' & could be seen by anyone & available online forever

DISCUSS the kind of things they see online – they might be looking for more information about their changing bodies & exploring relationships for example

HOLD the line on letting your child sign up for services like Facebook & YouTube that have a minimum age limit of 13

Do You Know The Apps Your Child Is Using?

Facebook - social networking site. Age limit to open an account is 13. Beware of accepting friends you don't know & bullying

Twitter – microblogging site for posting images/info (Tweets). Beware of malicious or bullying tweets, and not clicking on links that could be hoax

What's App – messaging app with minimum age limit of 16 to open an account. Can post images/information

TikTok (originally called musical.ly) is a social network for sharing user-generated videos,. Users can create and upload their own videos where they lip-synch, sing, dance, or just talk. Age limit is 13.

Snapchat photo sharing app that lets users share their photos for a few seconds before they 'disappear'. Heavily criticised for making it easy for children to be stalked or groomed. Age limit to open an account is 13.

Instagram Photo-sharing site, age limit to open an account is 13. Images can easily become public and once uploaded remain online

You Tube Video-sharing site, age limit to open and account is 13. Content of videos is often inappropriate for young children

bebo Recently relaunched, renowned for people posting inappropriate drawings – as well as the other potential issues common to social networking sites. Monitor closely if your child shows any interest in the 'new' Bebo.
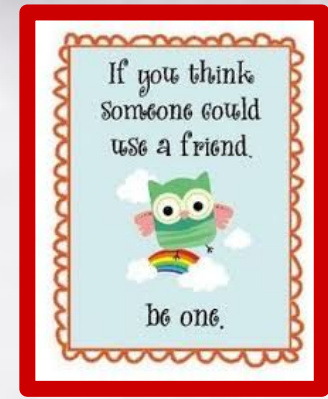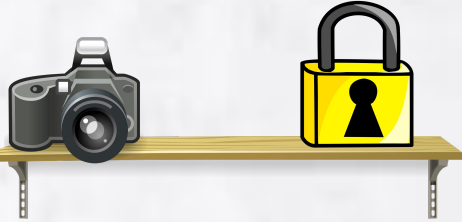
iMessage / Text – sending messages or photos between devices. Beware of cyberbullying

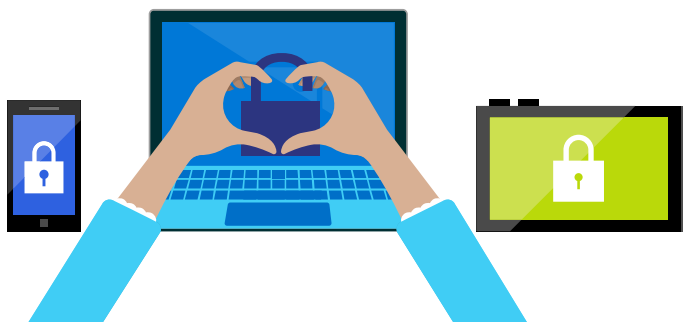**HABBO** Used to be called Habbo Hotel, and is a social networking site aimed at teenagers, although we know of children as young as 8 years old who use it. Adult content is easily accessible

ask.fm On Ask.fm, anonymous users ask other users questions. This means that they can easily hide their identity and effectively, say what they like without any consequences. Age limit is 13 to open an account

Top Tips for Online Safety

1. Protect your devices and accounts

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 updatw. Install legitimate antivirus and antispyware software. Never turn off your firewall. Protect your wireless router with a password, and use flash drives cautiously.
- Think twice before you open attachments or click links on email, instant messages or on social media, even if you know the sender.
- Lock your phone with a PIN to prevent others from making calls, texting, or accessing your personal information.
- Microsoft can help your family implement these and other suggestions at **microsoft.com/safety.**

2. Be a good 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.

Free online safety resources

For additional free online safety resources for educators, students and parents, visit:
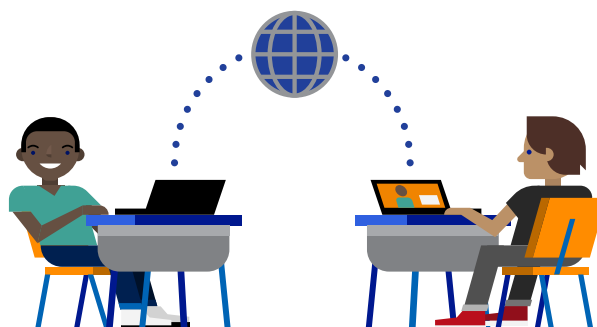
http://ikeepsafe.org/

3. Share with care

Information you share online about yourself or comments you post can become public. Additionally, 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.

- Avoid taking or sharing suggestive photos or videos. You can never fully control where they might end up.
- Make your social network pages private. Look for the **Settings** or **Options** area on your social media sites to manage who can see your profile, who can find you, who can tag you in photos, and who can make comments.
- Be proactive about blocking people you find offensive.
- Create profile pages and email addresses that aren't suggestive and don't reveal anything personal.
- Be choosy about adding new friends on phones or social sites, or in games.

4. Connect honestly and carefully

- Comply with copyright laws. Downloading copyrighted music or video games is illegal. And pirated files are often used to distribute viruses and spyware without the user's knowledge.
- Stay away from copying text from the web or buying finished essays or reports online.
- Only join social media sites that are appropriate 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.

For more tips and information on being a good digital citizen, visit:

https://aka.ms/msdigcitdocs

Content contributer

iKeepSafe
Generation Safe