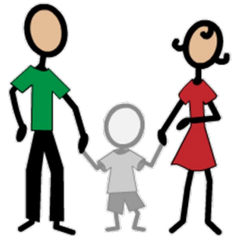
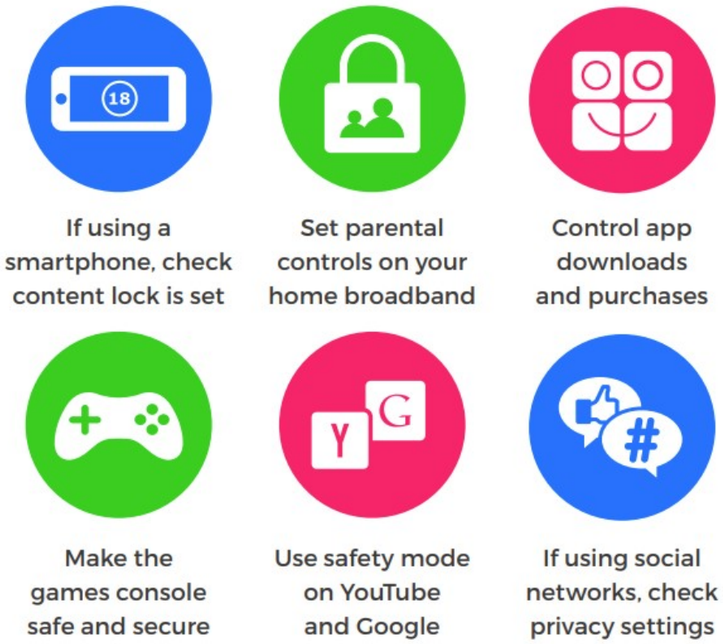
Parents



Get in control of parental controls



internet matters.org

https://www.internetmatters.org/parental-controls/smartphones-and-other-devices/

Mapledown School

Online Safety

Tips and website guides for keeping you and your family safe online

Keep your computers and mobile devices up to date. Turn on automatic updates to receive the latest security software. This helps protect your devices against viruses and online threats. Make sure your mobile/tablet apps are always up to date, e.g. Whatsapp. Use antivirus software to detect online threats and provide protection.

It's tempting to set one **password** for everything. This makes life easier for you, but also makes it easier for others to steal personal information from you. **Set different passwords for different areas of your online life**. A strong password is longer than eight characters in length and includes a mix of upper and lowercase letters, numbers and special characters. Scan this QR code for Do's and Don'ts.

Avoid clicking on links or opening attachments in unexpected emails, e.g. from your bank, energy supplier or even your friend. Contact them separately to find out if the email is genuine.

Phishing scams use fraudulent emails and websites to trick us into disclosing private account information or installing malware on our devices.

Only click on an email link if you are expecting it e.g. you've just ordered something from a company online or you've just signed up for an account on a website.

If you are asked to log into a website, go directly to the app or official site instead.

Keep personal information personal. Hackers can use social media profiles to figure out your passwords and answer those security questions in the password reset tools. Lock down your privacy settings and avoid posting things like birthdays, addresses, mother's maiden name, etc. Be wary of requests to connect from people you don't know.

When connecting to **public Wi-Fi** networks, be cautious about what information you are sending over it. Don't use public Wi-Fi to sign in to any app or website that contains your personal information.

Shop safely. Check website addresses when banking online or making purchases. The address should always start with "**https**" instead of just "**http**" and have a **padlock icon** in the website address field. This indicates that the website is secure and uses encryption to scramble your data so it can't be intercepted by an identity thief.

Protect yourself from malware apps, especially on Android devices. They can steal your contact details, hijack your login info from banking apps, read your messages, redirect your browser to fake sites and make themselves hard to delete. Scan this QR code for safety tips.

Children

11-15 year olds use on average 5 different websites and apps to communicate with friends at home, the most popular being Instagram

Whatsapp Snapchat Instagram YouTube

If your child is using these networking sites and respective apps, get up to speed on how they can manage their privacy settings with these "How to guides".

internet matters.org

https://www.internetmatters.org

NSPCC

https://www.nspcc.org.uk

childline

https://www.childline.org.uk/

mumsnet

https://www.mumsnet.com/