



Online Safety

Key Words

- Passwords** – A secret word or phrase that must be used to access certain things.
- Private** – Something which must be kept to yourself, and not shared with anyone.
- Personal Information** – Information that is related to you. For example, your name, address, post code and where you go to school.
- True/False** – Accurate or real information is true. Made up or wrong information is false.
- Internet** – Accessed by a device such as an iPad or Computer. The Internet holds lots of information, games, videos and files, and allows communication.
- Safe** – When you are protected from danger or harm.
- Online** – Connected to a computer or device (e.g. phone) that has internet access.
- In Real Life** – I met my friend In Real Life (IRL) at school yesterday. Not somebody that you talk to through the Internet and have never met.
- Social Networks** – A website or application (app) that allows people to talk with other people.
- Age Restrictions** – An official rule about the age someone has to be before they are allowed to do something. An example is that in the UK somebody has to be 18 or older before they are allowed to vote.
- Click Clever Click Safe** – The 'Click Clever Click Safe' campaign has three simple rules to follow. Zip it, Block it, Flag it. We can remember this as it will keep us all safe online.
- Bullying** – When one person, or a group of people, are repeatedly mean/nasty/unkind to a person.
- Cyberbullying** – When one person, or a group of people, are repeatedly mean/nasty/unkind to a person online e.g. through email, texts, Facebook, etc.
- Digital Footprint** – A digital footprint is a trail of data you create while using the Internet. It includes the websites you visit, emails you send, and information you submit to online services.
- CEOP** – A way or reporting something online.
- Consent** – Permission for something to happen or an agreement to do something.
- Social Media** – Websites and applications (apps) that enable users to create and share content or to participate in social networking.
- Protect** – Keeping yourself as safe as possible online.
- Tell** - If you see something online that makes you upset or uncomfortable, **talk to an adult you trust.**

Where to go for further information...

- <https://scib.info/children/>
- <https://www.childnet.com/parents-and-carers>
- <https://www.nspcc.org.uk/keeping-children-safe/online-safety/>
- https://www.thinkuknow.co.uk/4_7/



Top Tips

1. Be careful what you share
Once something is online, it's out of your control. If you don't want strangers to see it, don't post it.
2. Don't meet people you don't know in person
Even if you get on with them online, you never know who they really are.
3. Use a complex password
It should be hard for other people to guess your password and it's a good idea to change it regularly.
4. Check your privacy settings
Check who can see what you post and whether your accounts are public or private.
5. Talk about it
If you see something online that makes you upset or uncomfortable, **talk to an adult you trust.**

Phishing

- Very often, phishing is done by email. These emails appear to come from a bank, or other service provider.
- These emails allow criminals to get access to bank accounts and other personal accounts online.
- It usually says that because of a change in the system, the user needs to re-enter their usernames/passwords to confirm them. The emails usually have a link to a page that looks almost like that of the real bank.

GOV.UK

The government has taken urgent steps to list coronavirus as a notifiable disease in law

As a precaution measure against COVID-19 in cooperation with National Insurance and National Health Services the government established new tax refund programme for dealing with the coronavirus outbreak in its action plan.

You are eligible to get a tax refund (rebate) of 128.34 GBP.

[Access your funds now](#)

[The funds can be used to protect yourself against COVID-19] (<https://www.rls.uk/conditions/coronavirus-covid-19> precautionary measure against corona)

At 6:15pm on 5 March 2020, a statutory instrument was made into law that adds COVID-19 to the list of notifiable diseases and SARS-COV-2 to the list of notifiable causative agents.

From Government Gateway

This is an automatic email - please don't reply.

Passwords

- Passwords keep your personal information safe; this is why it is so important to make sure you have a strong one.
- Passwords should be something personal to you and easy to remember, but difficult for someone else to figure out.
- Avoid using the same password for every account and using your name, birthday, phone number, star sign etc, as these can easily be found out by other people.

Sharing Online

- When you choose a profile picture for a website, avoid photos that could give people you don't know information about where you live.
- Check your privacy settings regularly.
- Think about what should be shared in public and what should be kept private.
- Turn off location settings to help protect your privacy.
- Take care of your **digital footprint.**

Pegi Ratings



Remember to check Pegi ratings of games and websites! Most websites, including social media, have age restrictions. Make sure you are aware!

S

Stay Safe

Don't give out your personal information to people / places you don't know.

M

Don't Meet Up

Meeting someone you have only been in touch with online can be dangerous. Always check with an adult you trust.

A

Accepting Files

Accepting emails, files, pictures or texts from people you don't know can cause problems.

R

Reliable?

Check information before you believe it. Is the person or website telling the truth?

T

Tell Someone

Tell an adult if someone or something makes you feel worried or uncomfortable.

Follow these SMART tips to keep yourself safe online!

© Teaching Internet Safety www.teachinginternet.com