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**.

Passwords

Keep your password secure, do not share with your friends, and choose a screen name or username that is suitable, but does not give away any personal information.

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.**

CEOP

Remember

If something doesn't feel right, tell someone you trust.

All social networking sites and YouTube have 'report' buttons, use them!

CLICK CEOP
Internet Safety

Report to CEOP if you are worried about anything online.

ZIP IT
Keep your personal stuff private and think about what you say and do online.

BLOCK IT
Block people who send nasty messages and don't open unknown links and attachments.

FLAG IT
Flag up with someone you trust if anything upsets you or if someone asks to meet you offline.

Stay **Safe**
Don't give out your personal information to people / places you don't know.
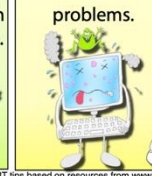
M Don't **Meet Up**
Meeting someone you have only been in touch with online can be dangerous. Always check with an adult you trust.

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

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

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

Follow these SMART tips to keep yourself safe online!

SMART tips based on resources from www.thinkuknow.co.uk
© Teaching Ideas