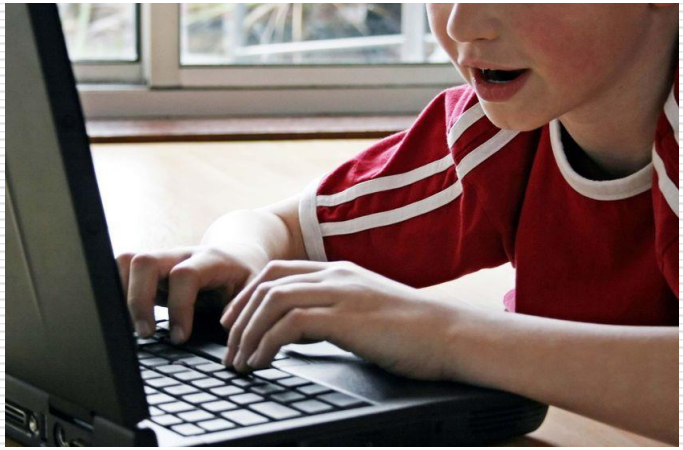
E-safety & becoming 'Digital Citizens'

Helping to keep your child safe online

HANDFORD HALL PRIMARY SCHOOL

15TH February 2022



What is E-Safety?

- E-Safety is fundamentally about ***educating*** children and young people to enjoy use technology safely.
- E-Safety is about ***learning to understand*** and use new technologies in a positive way.
- E-Safety is less about restriction and more about **education** about the ***risks*** as well as the ***benefits*** so we can feel confident online.
- E-Safety is concerned with ***supporting children*** and young people to ***develop safer online behaviours*** both in and out of school.

The National Curriculum

Key stage 1

Pupils should be taught to:

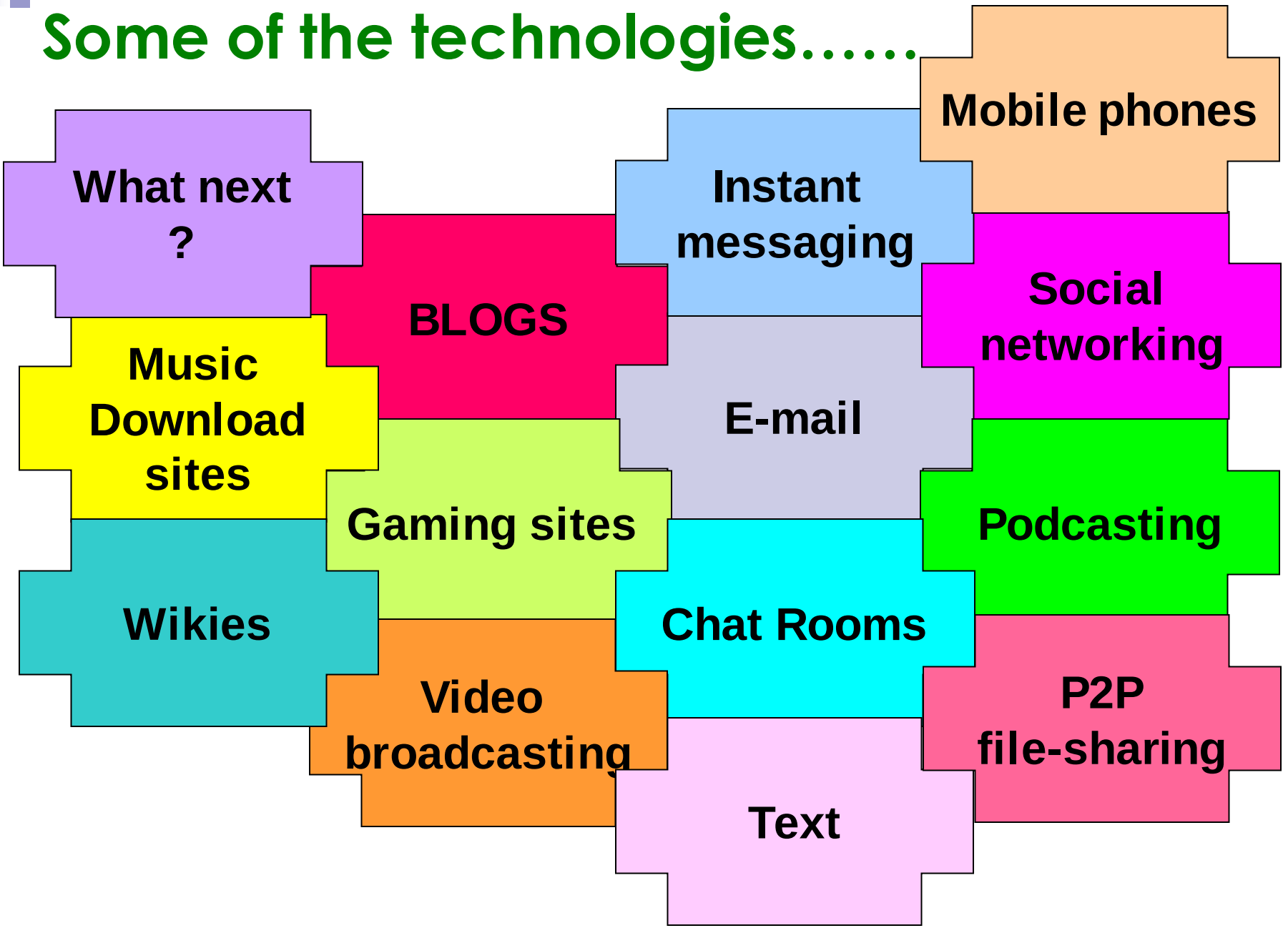
•Use technology safely and respectfully, keeping personal information private; know where to go for help and support when they have concerns about material on the internet.

Key stage 2

Pupils should be taught to:

•Use technology safely, respectfully and responsibly; know a range of ways to report concerns and inappropriate behaviour.

Some of the technologies……



Statistics

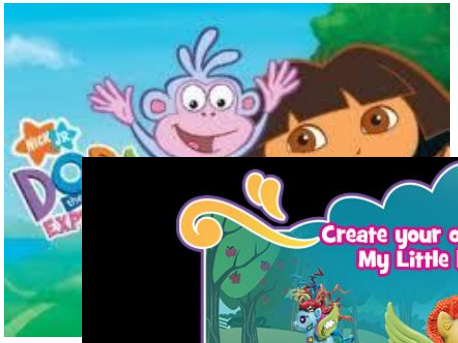
- 23% of 8 to 11 year olds & 72% of 12 to 15 year olds has a social media profile.
- 54% of 5-7s and 73% of 8-11s watch YouTube on a regular basis.
- Use of SnapChat has increased to 51% of 12-15 year olds.

(Ofcom: Children and Parents: Media use and attitudes report 2016)

- 1 in 3 internet users are children.
- 1 in 4 children have experienced something upsetting on a social networking site.
- 1 in 3 children have been a victim of cyberbullying.
- Almost 1 in 4 young people have come across racist or hate messages online

What is changing for children?

- One in four children under eight owns a tablet.
- One in 10 children has a mobile phone before they're five.
- 74% of eight- to 11-year-olds has access to a tablet at home.
- 63% of children have a smartphone before they start secondary school.
- 23% of children are seen on the internet before they're born.



Disney


MINECRAFT


Create your own Pony with
My Little Pony POP!
PLAY NOW


PLAY


neopets


stardoll


The SIMS 3
seasons
WIN
MAC


PLAYROOM
DECORATING
CATALOG
EVENTS
MUSIC

School approach to E-safety

Safe: keeping personal information safe

Meeting: online friends are strangers

Accepting: be aware of viruses

Reliable: information may be untrue

Tell: inform an adult

What can you do at home?

Talk to your child about the internet use.

- Get them to show you the sites they like to visit and look at the parents section to see what safety they have in place.
- Discuss with your child who it is safe to talk to and what information they can/cannot share.
- Talk through who their "friends" or "contacts" are - stress to your children that people they meet online are not always who they say they are.
- Explain that anything shared online or by mobile phone could end up being seen by anyone.
- As a family set clear rules about the use of social media and chatrooms.
- Keeping children's social media passwords and checking their use or become a member yourself for monitoring purposes.
- Tell children what they should do if they become worried or concerned.

What can you do at home?

- Changing your internet security settings to not allow children access to sites which may put them at risk.
- Use filtering software to block inappropriate sites.
- Make sure you have parental controls set up on all your devices – iPad, TV, console etc.
- Set up parental controls with your Internet Service Provider: One option your ISP can provide is the ability to limit the hours your child can access the internet e.g. not after 8pm.
- Block pop –ups and use SPAM filters, and your good judgement!
- Use a child friendly search engine e.g. Google Safe Search
- If they have a mobile phone turn off the GPS and consider restricting internet access on the phone.

WHATSAPP

- Interesting - not 13 this time…
- **Age requested is 16.**
- Location services can send details of your child's location with any image or message sent.
- No set parental controls but can be limited to 'My Contacts'.
- Does have facility to report spam and block unknown and known users.

FACEBOOK

- **Age limit of 13** once again.
- Very easy to get round, simple maths and you're in.
- Privacy settings are vital - settings need to be altered to select who can see your posts.
- Very easy to find - even in closed groups.
- Parental controls can be set via Windows and IOS but not through Facebook itself.

SNAPCHAT

- **Legal age requirement - 13** - should the 'correct' year of birth be entered they will be redirected to SnapKidz.
- No parental controls - SnapChat simply advise children to block users.
- Pictures don't really disappear.
- Location data - some features require location services.

Age Restrictions for Social Media Platforms

What is the minimum age for account holders on these social media sites and apps?

Under 13

- Roblox
- PopJam
- FaceTime

13+

- Twitter
- Facebook and Messenger
- Viber
- WeChat
- Monkey
- Yubo
- Dubsmash
- Instagram
- TikTok
- Skype
- Google Hangouts
- Reddit
- Snapchat
- Pinterest

16+

- WhatsApp
- Telegram Messenger
- Tumblr

17+

- Line
- Sarahah
- Tellonym

18+ or 13 with parent's permission

- YouTube
- WeChat
- Kik
- Flickr
- Play Store
- Spotify (12 with parental permission)

Sourced from NSPCC website October 2019

HOW MUCH DO YOU KNOW?

- How many actually know what their child is accessing online?
- Are all the contacts in a child's phone people actually known to them?
- If they're not, who are they? Location services alert!
- How much time is spent on live & instant apps?
- How many apps are you aware that your child has access?
- How many apps are they actually using?
- Have you set up parental controls on internet access at home?
- How often do you check browsing history?
- How comfortable are you with your child having an account below the required age?

HOW DO YOU APPROACH IT?

- Keep communication lines open - if you are not talking to a young person, you cannot support them
- Keep yourself informed - use the internet yourself, be aware of the issues, and know where to go to find support and help
- Be ready to start the conversation - even about difficult topics like grooming, pornography, online bullying, downloading and other illegal activity
- Make rules and agree them - it is also crucial to explain the reasons for rules, and challenge young people's preconceptions (that they won't get caught, e.g. or that they're too clever to be caught out by a groomer)
- Beware of blocking and banning - you may drive the young person to a riskier access point.

PRE-SCHOOL

- How many actually know what their child is accessing online?Set Parental Controls
- Set limits on how long they can spend online and use safe search options.
- Ensure your phone has passwords/pins.
- Assess the suitability of what your child is viewing – apps/films/websites.
- Think about your child's digital footprint.

AGES 4-6

- How many actually know what their child is accessing online?
- Difference between online & offline.
- Parental Controls.
- Review suitable websites.
- Passwords & Private information.
- How to behave online.
- Enforce Gaming & Digital Time limits.
- Public WiFi may not have parental controls. Use 3G/4G to avoid Public WiFi scams.

AGES 7-9

- Use Parental Controls on all devices including games consoles.
- Understand Fake News – Safe Searching use Safe Search on Google etc.
- Ensure they understand not to reveal private info – school, address etc.
- Review your list of suitable websites/apps/games for your child to use.
- Time Limits.
- Ensure they understand what a stranger is and dangers of meeting people who are online.

AGES 10-12

- Review Parental Controls.
- Smartphones- remember you pay the bill!
- Set family rules on use of all devices.
- Ensure child understands privacy settings even on photos.
- Check apps they have e.g. Live Streaming.
- Ensure they understand the consequences of what you put online.
- Exploring relationships and how they look become far more important. Ensure you have explained how people can behave.
- Check they understand the implications of adding people never met in real life to their contacts and how their location can be viewed by them if Location Based Services is not off.
- Ensure they know how to turn off Geo-tag on photos.

AGE 13+

- Ensure that you have explained how people behave online and the consequences – Bullying, Sexting etc.
- Ensure they know the importance of a positive digital footprint re: University and Employers.
- Ensure they understand how to spot dodgy e-mails and scams.
- Keep a dialogue going between you and your teen.
- Social Media accounts – ensure you understand what you are signing up to, check you understand privacy settings and how to restrict who views your profile and pics.

How to disable GPS geolocation

- On an iPhone or iPad Launch the Settings app from your Home screen. Tap on Privacy. Tap on Location Services. Tap on Camera. Choose Never.

- On Most Android phones Open the camera app and tap settings Scroll down to ‘geo tag’ or ‘location tag’ Select disable/off

How to disable GPS geolocation

On Facebook

Open your profile page Click on the ‘more’ button below profile picture

Select View privacy shortcuts

Select more settings

Click Location

Find location history and turn off

- phone location services for Facebook can also be turned off using the privacy tab under phone settings.

What is Cyberbullying?

- Sending cruel, nasty, or threatening messages by text or computer
- Creating websites or fake profiles, or adding to existing websites, unpleasant stories, pictures, or jokes making fun of others.
- Posting pictures or video clips online without the person's knowledge
- Breaking into another person's e-mail/social network/msn account and sending nasty or embarrassing material to others.
- Using Instant Messaging services to gang up on or exclude another person.
- Racist, Xenophobic and Homophobic comments posted online or sent by text

What to do if your child is being bullied online…

- Don't reply/retaliate

- Report it to the school

- If on a social networking site, report them to the website and BLOCK/DELETE the *user*.

- Report it to the police (through the CEOP button available on the CEOP website)

- SAVE the conversations, do not delete any evidence.

For more information…..

- http://www.parentscentre.gov.uk/
- www.thinkuknow.com
- http://www.getnetwise.org/
- http://www.childnet-int.org/
- http://www.bbc.co.uk/webwise/
- http://www.iwf.org.uk/
- http://www.internetmatters.org/age-guides/videos.html
- http://facebook.com/safety