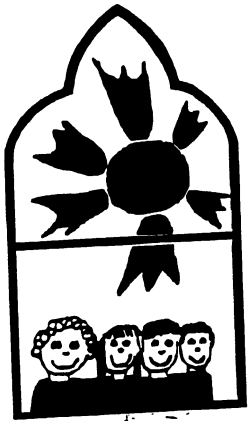# Online Safety

Safer online use
Parent presentation

Ashton Gate Primary School

<u>Aims of presentation</u>

- Raise Online Safety awareness
- Highlight potential issues
- Practical tips
- Reporting and support

Technology continues to change the way we live, work and play. We recognise that today's generation learn and engage differently to students in the past and that schools need to adapt and change to reflect the wider changes in society.

To help us to use technology to its full potential, we must understand the positive and negative aspects of its uses.

Online Safety is not about technology, it is about our behaviour and the behaviour of other people.

24% of 3-4 year olds have access to a tablet in the home. 1% have a social media profile (likely set up by someone else)

71% of 12-15 year olds have their own social media. 89% of children this age watch YouTube for around 11 hours a week

There is a huge jump in the number of children owning a phone when they get to 12 as they move to secondary school. We are increasingly seeing children younger than this having one too.

ces that

net

Video

https://www.youtube.com/watch?v=2IcpwISszbQ&safe=active
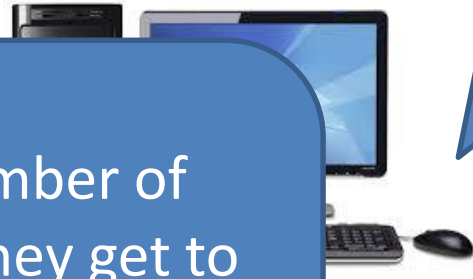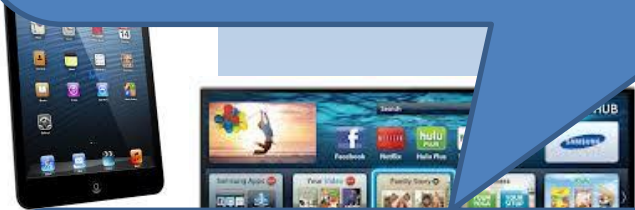
What are the main concerns about the Internet?

- Gaming

- Privacy

- Cyber security

- Online harm

- Live streaming

- Persuasive design

- Fake news

- Pornography

Gaming

- Gaming is a huge industry and has been for a long time.
- Statistically most 'gamers' are adults, although there are of course games aimed at children.
- Gaming is not just a male past time.
- Gaming has possibilities of becoming a career now.
- Although gaming has potential to become negative if perused as only interest, it is not necessarily a bad thing.
- Gaming can be a good way to avoid isolation for children.
- Gaming can be a way to connect with friends from school etc.
- Increasingly gaming has become a way to make new friends.

Privacy

- Digital sharing – adults and children to be aware of what is good and bad to share.

- Awareness of what other people would like shared – e.g. not publishing photos of other people without their consent.

- Most apps collect your data. Think before signing up to new apps.

- Smart speakers always listening and storing recordings. Be aware of and use the mute button.

- Younger people will have more of their data collected than previous generations. Their digital footprint will be larger as it will have started at a younger age.

Cyber security

- Data breaches and hacks – many high profile.
- www.testmyprivacy.com website to check if your passwords have been collected.
- Passwords can be replaced by a sequence of words.
- Teach children not to give out personal information (name, age, address, passwords)
- Think before opening emails and attachments.
- Think before signing up to something.
- Speak to an adult if you make a mistake – praise for asking for help.

Online Harm

- SELMA – hacking hate.
- Tackling and recognising hate speech.
- Online harm could be to an individual or a group. Both should be reported to an adult.
- Revenge porn – prevalent in secondary school (though improving) so good to teach children at a young age to be responsible with images of themselves, and to not share images of other people.

Live streaming

https://www.youtube.com/watch?v=0EFHbruKEmw

- Something used in our everyday lives (e.g. Skype, FaceTime)
- Increase of time spent online involving video.
- People live stream their everyday lives as well as important events.
- People see constant live streams and they might not always reflect real lives of the people they are watching.
- Live streams can be recorded. Young people may use technology to live stream within relationships without realising the videos are being saved. This is an area young people are becoming more aware of these issues and more vigilant, though we still need to continue educating them on potential dangers.
- People may be blackmailed if their webcam has been hacked.
- Revenge porn helpline – positive information to try and tackle the situation without judgement.

Persuasive design

- Red circular alerts – shape and colour subliminally tells us to stop and take notice.

- Three dots – waiting for messages.

- Infinite scrolling – you can't get to the end of Facebook or Twitter feed.

- Scores relating to response times on Snapchat.

- Lots of subliminal manipulation to keep your eyes on the screen as much as possible.

Fake News

- Propaganda – news with a political agenda.
- Clickbait – designed to suck you in and keep you there.
- Sponsored content – advertising made to look like news – not always easy to distinguish.
- Satire and humour - varies in quality and intention. Starts as being intended as a joke and could backfire or snowball.
- Error – established news organisations make mistakes.
- Partisan – ideological and may contain emotional or passionate language
- Conspiracy theory – not always falsifiable but also not easy to prove. Rejection of experts.
- Pseudoscience - purveyors of miracle cures, anti-vaccination, climate change denial etc. Misrepresents real scientific studies with exaggeration or false claims.
- Misinformation – could be a mix of truths and falsehoods. Author may not be aware the content is false.

Pornography

- Sexting – becoming a normalised part of life for adults. Children will often experiment before they are ready to understand.
- Could be entirely unsolicited. May or may not include images or videos.
- Children may see pornography by mistake – e.g. using an adults laptop or a friend showing them.
- Creates a false representation of healthy sexual relationships.
- Normalises behaviours that we wouldn't want our children to be aware of.
- May be a part of sexual exploration if children don't feel confident asking for information. For example children wanting to come out but don't feel ready, but equally so with all young people.
- Creating an environment where children are able to speak to adults will give them the chance to ask questions without seeking answers through pornography.

Cyberbullying

https://www.youtube.com/watch?v=MV5v0m6pEMs

STOP.
BLOCK.
TELL.

'Cyber bullying is rife on the internet and most young people will experience it or see it at some time. In our recent national bullying survey, 56% of young people said they have seen others be bullied online and 42% have felt unsafe online. Cyber bullying can happen 24 hours a day, 7 days a week and it can go viral very fast.' *Ofcom*

Do you look after your Digital Footprint?

We have all heard of the term "digital footprints" but do we really understand what they mean?

- Essentially a digital footprint is data that is left behind when users have been online.

- Whatever we are doing on the internet we can leave a trail of information behind us which people can use to determine what we might be interested in buying, or for other less savoury purposes such as trying to hack into our online accounts and trying to access passwords etc.

- A lot of employers will also use social media to vet prospective employees so it is important that you are mindful as to what you post on any such sites.

- As the internet becomes bigger and bigger it is becoming increasingly important to think about what might happen to the ownership of the photos that you own and content that you write.

Remember that what [goes on the internet](#) normally stays there, even if you do delete posts there will be a trail of data that you have left behind

Age restrictions

http://www.net-aware.org.uk/

O₂ 😊 NSPCC Net Aware)))

Type and select network

🔍 (e.g. Facebook)   >

Explore all networks

A-Z   Most popular

Your guide to the social networks your kids use

Stay up to date and keep your child safe in today's digital world

Friending or communicating with people they don't know.

Grooming and sexual abuse.

Sharing personal information.

What do 'parent controls' do?

- Filter and block content you don't want your children to see – such as violence and pornography.

- Restrict information that can be shared.

- Set time limits on how long children are online.

- Control the time of day that children can access the internet.

- Set different profiles, so that each family member can access content that's appropriate to them
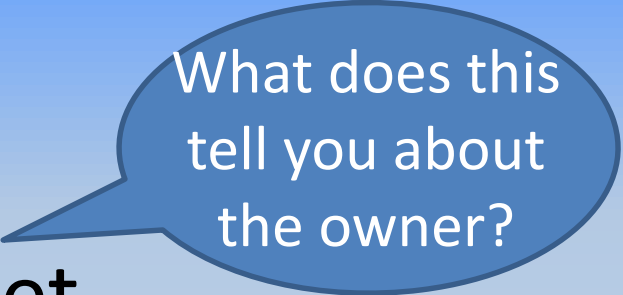
What can be done?

- Set up home broadband parental controls.

- Set controls on your search engine.

- Privacy settings.

- Block pop-ups.

- Keep talking.

http://www.internetmatters.org/controls/interactive-guide/

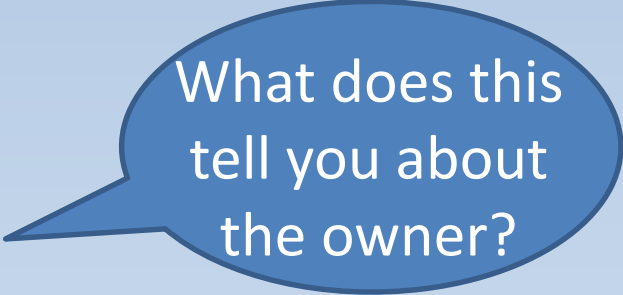https://swiggle.org.uk/ - child friendly search engine

Usernames

JoeSmith2005
SherlockBakerStreet

What does this tell you about the owner?

MinecraftFan
GuitarGod

What does this tell you about the owner?

Passwords

Recommendation now is to have a 'pass phrase' – A set of 3 or more words taken at random
e.g. panda grass bottle

How do I report an incident?

➢ Let school know

➢ UK Safer Internet Centre Parentport is home to the UK's media regulators and contains details on how to report, a range of online content, including advertising and games, that you feel may be unsuitable for children. www.parentport.org.uk

➢ For any indecent/racist content online contact Internet watch who will remove this.

➢ If you are suspicious of child exploitation / grooming contact the police branch CEOP – Child Exploitation and Online Protection Centre www.ceop.police.uk www.saferinternet.org.uk

➢ If in immediate danger call 999

What is the School doing?

- Regular teaching of online-safety issues through PSHE and computing curriculum.
- Giving children the tools to know how to keep themselves safe online.
- Exploring and acting out different scenarios.
- Giving children the responsibility and autonomy to make the right decisions.
- Safer Internet Day and Online-safety assemblies.
- School council raising awareness of online-safety issues.
- Online-safety tips on newsletters and digital parenting magazine.
- Staff and Pupil Acceptable Use agreement.
- Online-safety staff training.
- Online-safety policy.

How does the school deal with any Online Safety incidents?

- All Online Safety issues are logged.

- Online Safety group, including co-ordinators, safeguarding officers and Governor will be informed of serious issues.

- Relevant issues discussed in class.

- All school websites are filtered by Bristol City Council.

- New child friendly search engine used in school– accessible at home.

What can I do right now?

- Encourage your children to use nicknames instead of their full name online.

- Set up a family email address when signing up to a new game and websites.

- Create a family agreement to establish your children's boundaries and your expectations whilst on the internet.

- Show an interest in the games that they play.

- Encourage children to use the internet and gaming consoles, within a shared family environment.

- Maintain an open dialogue with your child and encourage them to talk about their internet use e.g. who they are talking to, services they are using and any worries they may have.

- Give your child strategies to deal with any on-line content that they are not comfortable with – such as turning off the screen, telling an adult they trust and using online reporting facilities.

- Read signs – are they upset after using the internet or mobile phone?

- Check privacy settings on all devices.

- Check the 'History' on the internet

- Contact the service provider for security measures.

- Report any concerns.

- If your child is being bullied online, **save** all available evidence and **report** the incident e.g. the school, service provider or police.

Where do we go for more information

https://www.parentport.org.uk/

Let's keep kids safe online

https://www.getsafeonline.org/

https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

http://www.internetmatters.org/controls/interactive-guide/

http://www.thinkuknow.co.uk/

http://www.kidsmart.org.uk/

http://www.net-aware.org.uk/

https://www.ceop.police.uk/

http://www.childnet.com/resources

If you have any questions please feel free to email them to either tom.hughes@bristol-schools.uk or jonathan.anderson@bristol-schools.uk

We will do our best to answer them, or point you in the direction of someone else who can.