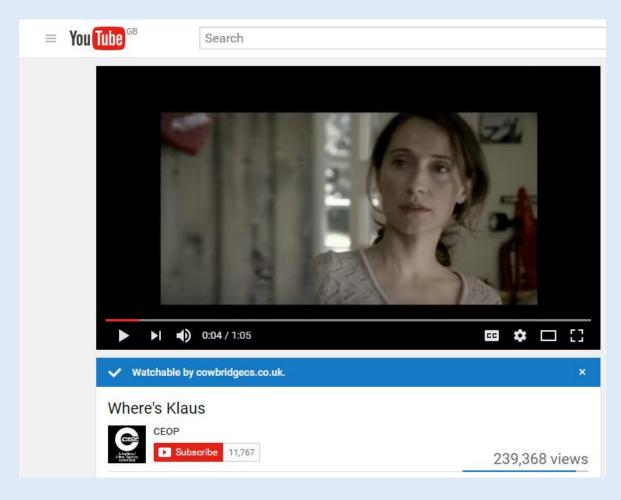


Safeguarding young people on the internet and related technologies.





https://youtu.be/-IOOn2wR8bU

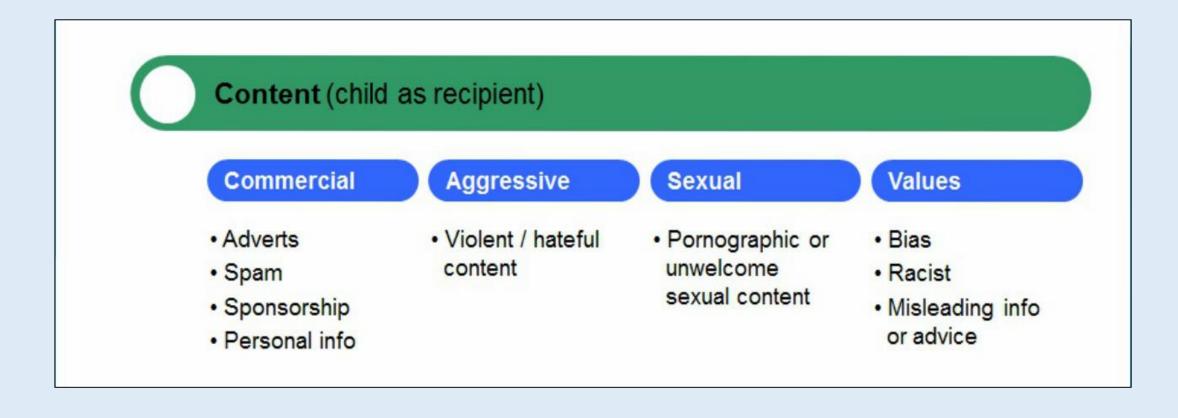


# What risks should we be guarding against?

Following information from the EUKids online project

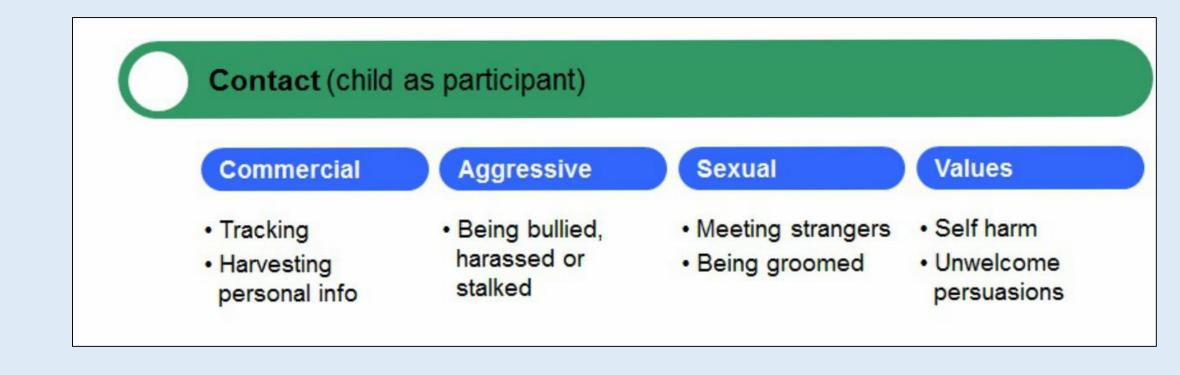


# What risks should we be guarding against?



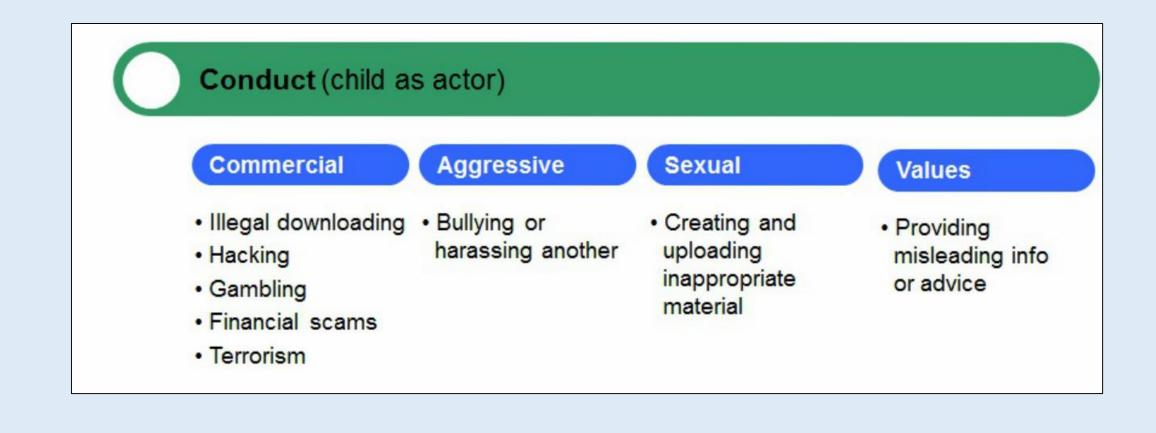


# What risks should we be guarding against?





# What risks should we be guarding against?





## Not just a problem for now

Your Digital Profile/Footprint



### Percent of recruiters and HR professionals who use these types of sites when researching applicants

Search engines	78%
Social networking sites	63%
Photo and video sharing sites	59%
Professional and business networking sites	57%
Personal Web sites	48%
Blogs	46%
News sharing sites (e.g. Twitter)	41%
Online forums and communities	34%
Virtual world sites	32%
Web sites that aggregate personal information	32%
Online gaming sites	27%
Professional background checking services	27%
Classifieds and auction sites	25%
None of these	2%



# Approach adopted by the School



#### Teachers and other staff

All staff receive training in E-Safety

but a general guideline for Cowbridge staff on being made aware of an E-Safety Issue:

- Manage pupil well being (reassurance, support of victim).
- Contact safeguarding officer immediately
- If possible and legal, save evidence.



## **Pupils**

All pupils receive continuous and age appropriate training in keeping themselves safe:



#### "Rules" that we emphasise in Key Stage 3.

- Never to agree to meet someone that you have met online. If you do not know the person in 'real life', tell your parents if they ask to meet you.
- Do not give out personal information about yourself online without your parent's permission. This includes your name, where you live or your telephone number.
- Talk to your parents first about pictures you want to post online, whether they be of yourself or your friends or family members.
- Do not respond to messages you receive that are mean or speaking meanly about others. Tell your parents about these messages.
- Do not give out any of your passwords to friends or anyone you meet online.
- Check with your parents first before downloading or installing any software on your computer.
- Ensure privacy settings are activated on all of social media websites you use.
- Always be kind of others online. Do not do anything that may hurt others including joining in conversations discussing other people's problems.
- Be careful about discussing details about your own personal problems with your friends online. It is better to speak to them in person. Tell your parents or teacher if you are struggling with something.



#### Video shown to Year 7 pupils



www.youtube.com/watch?v=kgCNGvL0g1g



#### Older Pupils – Social Media and Digital Footprint

- Think before you post anything
- Understanding your digital footprint
  - Search for yourself using Google or another search provider
- Appropriate language and behaviour
  - Consider how others may interpret your words, especially if using abbreviations
- Protect your passwords
  - Don't disclose and the stronger the better!



- Managing your Privacy settings, using privacy effectively
- Testing your privacy



- Find out from your friends what information they can see on your profile?
- Discussing expectations with friends
  - Are you happy to be tagged in a photo?
- Familiarise yourself with your organisations policies and procedures
  - Make sure you know how what the rules are!
- Know how to report an issue



# Suggested approach for Parents



#### What can I do right now?

Maintain an open dialogue with your child and encourage them to talk to you about their internet use: for example who they're talking to, services they're using, and any issues they may be experiencing. Create a family agreement to establish your children's boundaries, and your expectations, when on the internet. Give your child strategies to deal with any online content that they are not comfortable with - such as turning off the screen, telling an adult they trust and using online reporting facilities. Consider using filtering software to block unwanted content. In addition to filtering, remember that discussion with your child, and involvement in their internet use, are both effective ways to educate them about the internet. Encourage your children to 'think before you post.' Online actions can impact not only yourself but the lives of others. Content posted privately online can be publicly shared by others, and may remain online forever. Understand the law. Some online behaviour may break the law, for example when downloading or sharing content with others. Be able to recommend legal services. Familiarise yourself with the privacy settings and reporting features available on popular sites and services. If your child is being bullied online, save all available evidence and know where to report the incident, for example to the school, service provider, or the police if the law has been broken. Familiarise yourself with the age ratings for games and apps which can help to indicate the level and suitability of the content. Also see if online reviews are available from other parents as these may be helpful. Set up a family email address that your children can use when signing up to new games and websites online. Encourage your children to use nicknames (where possible) instead of their full name online, to protect their personal information, and create strong passwords for every account. Supporting Information and advice Set up a PIN or password on devices to help protect personal information. for parents youna

and carers

people

online

Sign up to our Childnet newsletter at www.childnet.com.



Help make sure that your children know how to stay safe online, by using our SMART Rules for primary aged children, or 5 Tips for Teens.

#### 5 SMART Rules for primary aged children:

### Safe: Keep safe by being careful not to give out personal information when you're chatting or posting online. Personal information includes your email address, phone number and password.

- Meet: Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present. Remember online friends are still strangers even if you have been talking to them for a long time.
- Accepting: Accepting emails, messages, or opening files, images or texts from people you don't know or trust can lead to problems they may contain viruses or nasty messages!
- Reliable: Someone online might lie about who they are and information on the internet may not be true. Always check information by looking at other websites, in books, or with someone who knows. If you like chatting online it's best to only chat to your real world friends and family.
- Tell: Tell a parent, carer or a trusted adult if someone, or something, makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

#### 5 Tips for Teens:

- Protect your online reputation: use the tools provided by online services to manage your digital footprints and 'think before you post.' Content posted online can last forever and could be shared publicly by anyone.
- Know where to find help: understand how to report to service providers and use blocking and deleting tools. If something happens that upsets you online, it's never too late to tell someone.
- Don't give in to pressure: if you lose your inhibitions you've lost control; once you've pressed send you can't take it back.
- Respect the law: use reliable services and know how to legally access the music, film and TV you want.
- Acknowledge your sources: use trustworthy content and remember to give credit when using other people's work/ideas.

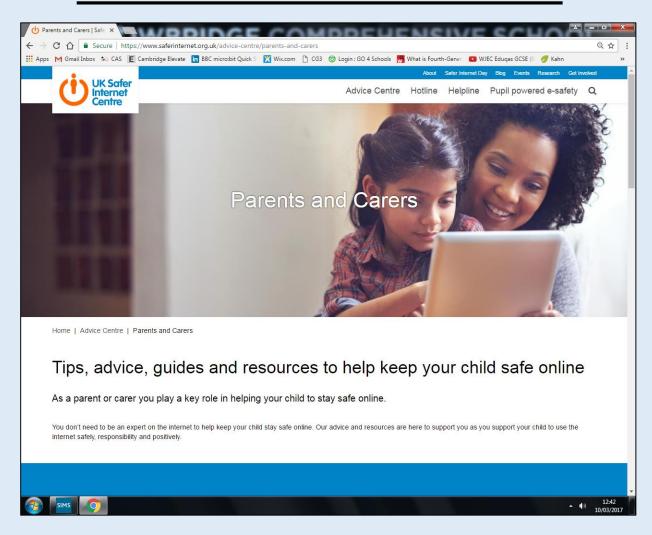




# Where to find more information



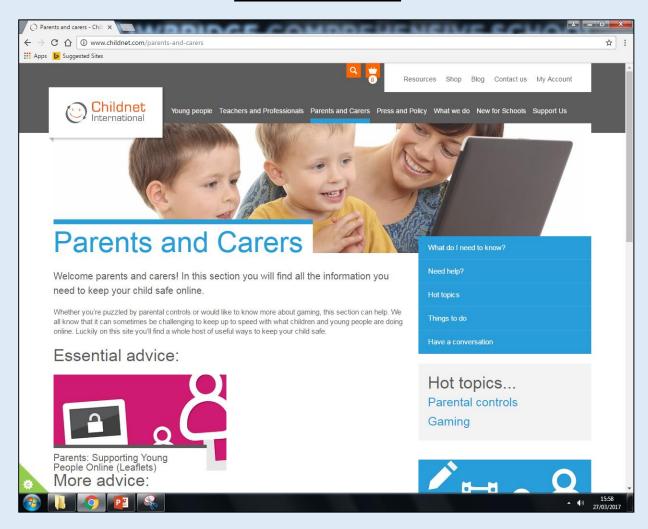
#### **UK Safer Internet Centre**



www.saferinternet.org.uk/advice-centre/parents-and-carers



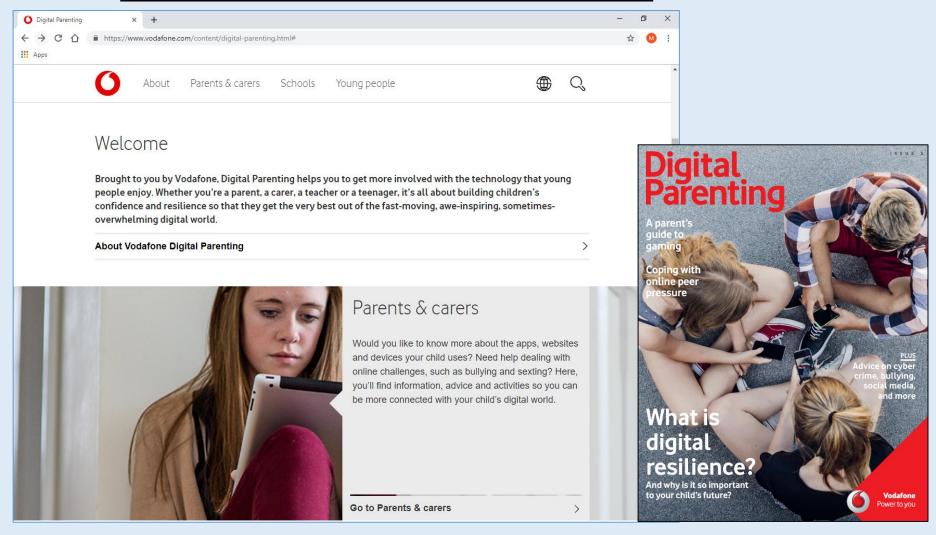
#### **Childnet**



www.childnet.com/parents-and-carers



#### **Vodafone Digital Parenting**



https://www.vodafone.com/content/digital-parenting.html