Tips for mobile phones

∗ Set parental controls where required– all smart phones have a restrictions section.

∗ Set mobile phone rules, e.g. no mobile phone in the bedroom at night.

∗ Before buying a phone, find out what functions it has.

Gaming

Keep a clean machine: Before your children start playing, be sure your computer has an activated security suite: a firewall, anti-spyware software and anti-virus software. Having the latest security software, web browser and operating system is the best defence against viruses, malware and other online threats.

Make their password a sentence: Be sure your children have strong passwords for their gaming accounts.

Remain positively engaged: Let your children know they can come to you if they feel uncomfortable when playing a game. Participate in the game with your children.

Check the rating: Checking for a game's Entertainment Rating Software Board's rating.

Empower your children to handle problems: Make sure your child knows how to block and/or report a cyberbully. Tell them to keep a record of the conversation if they are being harassed and encourage them not to engage the bully. You can also notify a game's publisher or online service about the offender.

Protect personal information: Make sure your child's user name does not give away their real name, location, gender, age or any other personal information.

Protect your identity: If your children are playing a game that features live voice chat, make sure they are disguising their voice. If the game does not have this feature, do not let them use voice chat.

Limit their time playing games: Some consoles offer parental control features that let parents decide when and for how long their child can play, who they can play with, or even let you "mute" or disable the ability for your child to hear the game's online chat (which can at times be pretty colourful).

Keep the computer out in the open: If your computer is in a central location, you can monitor your children's online activities.

Explain privacy: Make sure your children know that they may not send out any materials to fellow gamers that contain private information and/or data.

Enable parental controls: Use built-in parental controls on your Web browser.

Don't let your children download anything without your permission

Prohibition won't work: Your children will use computers and games consoles, even if it's at school or at friends' houses. If you talk to your kids about risks and good judgment, they will be able to get a lot more out of the web.

What to do if things go wrong

Children can visit the Thinkuknow website (www.thinkuknow.co.uk) and report issues by clicking on the report abuse icon:

All reports are taken seriously and will be followed up. Many Social Networking sites and IM applications will also have the facility to report inappropriate content. For example Facebook has a 'Report' link on each page or concerns can be e-mailed to abuse@facebook.com and Bebo has a 'Report abuse' link on every profile page and below every piece of content (ie photo, video etc).

As a parent you can make reports on your child's behalf by visiting the parent's section of the CEOP website (www.ceop.gov.uk)

Useful websites

There are a range of useful websites that provide information for parents and children:

www.thinkuknow.co.uk

www.digizen.org

www.childnet.com

www.ceop.gov.uk

www.getsafeonline.org

www.dcsf.gov.uk/ukccis

http://www.saferinternet.org.uk/advice-and-resources/parents-and-carers

But most importantly....

Remember that using technology can be a wonderfully powerful and positive experience. We should not discourage its use but support youngsters and help them to use it safely.

Internet Safety Practical Advice for Parents

- Always sit with children at this age when they are online

- Create a personalised online environment by limiting children to a list of favourites or "bookmarked" sites.

- Use child-friendly search engines or one with parental controls

- Keep internet– connected computers in an open area where you can easily monitor children's activities

- Investigate internet-filtering tools as a complement– not a replacement– for parental supervision.

- Start teaching kids about privacy. Tell them never to give out information about themselves or their family when online.

- Have children use an online nickname if a site encourages them to submit their names to 'personalise' the web content.

- Protect them from offensive 'pop-ups' by disabling Java on your computer or using blocking software.

- Don't let children this age use instant messaging, email, chat rooms or message boards.

Top 10 Tips for parents

1. Set up an account for each user on your pc at home and only give yourself administrator access. This will allow you to keep control of the settings and the installation of software. Each user account can be password protected.

2. Add a screensaver protected by a password to your account so that if you leave your pc for 5 minutes you will have to enter your password. You can do this in the 'Control Panel'.

3. Encourage your family to use technology in a public part of the house and not in a bedroom. This applies not just to pcs but also to laptops, game consoles, internet browsers on phones etc.

4. Remember that many consoles come with family settings. For example if you want to disable or limit 'Xbox Live' on an Xbox 360 you can do so by going to 'Settings, Parental controls'. There is also the option to add a mask to voices so that a youngster's voice sounds like that of an adult or even a robot.

http://support.xbox.com/en-GB/xbox-360/security/xbox-live-parental-control

https://support.us.playstation.com/app/answers/detail/a_id/5097/~/ps4-parental-controls

5. Use a pop up blocker. Both Internet Explorer and Firefox come with their own pop-up blockers. If you are accessing a site that has a genuine pop up window that you need to access you should add it to the trusted sites rather than turn off the pop up blocker. The settings can be found in the 'Tools' menu of the browser.

6. Encourage your child not to open e-mails from unfamiliar e-mail addresses and to avoid opening suspicious attachments. As far as possible you should encourage your child to use the school's Learning Platform as this provides a safer environment.

7. Ensure that your favourite search engine do 'safe searches'. This will make sure that a search returns content suitable for all ages. For example, to set Google to do safe searches click on search settings on the homepage and then ensure that moderate or strict filtering is enabled. Youtube also has a safe mode.

8. Adjust the security settings of your browser and pc. For example, Apple Macs allow users to change settings in the parental control preference pane. Windows Vista and Windows 7 also have parental control sections. Internet provider also have their own filtering which is free to set up.

9. Keep virus protection software up to date.

10. Engage in their world – add them as a friend on a social networking site, text them, discover what their games consoles do etc.

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.