

Online Safety for Governors





What are we going to consider this evening?



- Statutory responsibility for Governors
- The online world: What's it all about?
- Sites and devices used by children and young people including Instagram
- Risks children and young people face online
- Online vulnerabilities
- Tools available moderation, filtering, blocking
- Top tips and advice









Keeping children safe in education

Statutory guidance for schools and colleges

September 2016





KCSIE



Read and identify key responsibilities for Governors in the context of online safety?





Main Points



Governing bodies should be doing all that they reasonably can to limit the above risks from the school's IT system:

- Being exposed to illegal, inappropriate or harmful material
- Being subjected to harmful online interaction with other users
- Personal online behaviour that increased the likelihood of, or causes, harm





Other Considerations



- Ensuring that effective filtering and monitoring is in place without 'over blocking'
- A whole school approach to online safety
- Clear policy on the use of mobile technology in school
- Staff training this could be included within safeguarding training
- Online safety education for the young people





Statistics from the BBC February 2015



- More than half of children in the UK (57%) have done something "risky" or anti-social online, a poll of 2,000 11to 16-year-olds suggests.
- Almost two-thirds (62%) told the BBC Learning poll they felt under pressure from others to act in this way.
- Activities included sharing unsuitable videos or pictures of themselves or saying nasty things about others and looking at unsuitable websites.
- Some 20% said they had put pressure on someone else to act negatively online





Inspecting safeguarding in early years, education and skills settings

Guidance for inspectors undertaking inspection under the common inspection framework

This guidance is for use from September 2015 and remains in draft until that point. Minor amendments may be made to the text prior to September.

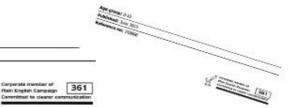




Age group: All

Published: June 2015

Reference no: 150067





The common inspection framework: education, skills and early years

Mandatok for respections samed out, respectively, sacker scales is of the bissisters act 2006 (be previously, section 109 of the Foundation and Subs Act 2006, the bissisters and improtons Act 2006, and the Disbland Act 2006.

The senses inspection framework with our from Disself regests marketined self-senses and ecologies, non-economics independent whose, further education and editing provision and ergotional only years settings in England.

The common imperition framework committee effect from 1 Textender 2015 and recision in draft until that point. Hiera ananother is may be made to the text prior to Seaten than

Online Safety

The term 'online safety' reflects a widening range of issues associated with technology and a user's access to content, contact with others and behavioural issues

P6 10

Safeguarding action may be needed to protect children and learners from:

- bullying, including online bullying and prejudice-based bullying
- the impact of new technologies on sexual behaviour, for example sexting

Adults understand the risks posed by adults or learners who use technology, including the internet, to bully, groom, radicalise or abuse children or learners. They have well-developed strategies in place to keep children and learners safe and to support them to develop their own understanding of these risks and in learning how to keep themselves and others safe.

Leaders oversee the safe use of technology when children and learners are in their care and take action immediately if they are concerned about bullying or children's well-being. Leaders of early years settings implement the required policies with regard to the safe use of mobile phones and cameras in settings.

Inspecting how effectively leaders and governors create a safeguarding culture in the setting



staff, leaders and managers understand the risks posed by adults or young people who use the internet to bully, groom or abuse children, young people and vulnerable adults; there are well-developed strategies in place to keep learners safe and to support them in learning how to keep themselves safe

staff, leaders and managers oversee the safe use of electronic and social media by staff and learners and take action immediately if they are concerned about bullying or risky behaviours

Arriving at judgements about safeguarding arrangements

inspectors will consider, among other things, children's and learners' understanding of how to keep themselves safe from relevant risks such as exploitation and extremism, including when using the internet and social media, inspectors should include online safety in their discussions with pupils and learners (covering topics such as online bullying and safe use of the internet and social media). Interpectors should investigate what the school of further education and skills provider does to educate pupils in online safety and how the provider on school doels with issues when they arise.

Inspecting and reporting on safeguarding concerns

Inspectors should ensure that they are aware of information available to the public, reported in the press or accessible on the internet, including that available on the early years setting, school or further education and skills provider's website, if available. This may contain information related to safeguarding. Inspectors should do a check on the internet as part of their preinspection planning to see whether there are any safeguarding issues that may need to be followed up during inspection. All evidence that relates to planning for the inspection should be recorded.



inspectors will consider, among other things, children's and learners' understanding of how to keep themselves safe from relevant risks such as exploitation and extremism, including when using the internet and social media. Inspectors should include online safety in their discussions with pupils and learners (covering topics such as online bullying and safe use of the internet and social media). Inspectors should investigate what the school or further education and skills provider does to educate pupils in online safety and how the provider or school deals with issues when they arise.

Inspecting and reporting on safeguarding concerns

Inspectors should ensure that they are aware of information available to the public, reported in the press or accessible on the internet, including that available on the early years setting, school or further education and skills provider's website, if available. This may contain information related to safeguarding. Inspectors should do a check on the internet as part of their preinspection planning to see whether there are any safeguarding issues that may need to be followed up during inspection. All evidence that relates to planning for the inspection should be recorded.

outstanding

- Whole school consistent approach
- Robust integrated reporting routines
- Effective staff development
- Clearly communicated and respected policy
- Progressive curriculum
- Secure and effective infrastructure
- Effective monitoring and evaluation

inadequate

- Personal data is unsecured
- Security of passwords is ineffective
- Policies are generic and not updated.
- There is no progressive, planned e-safety education
- There is no Internet filtering or monitoring.
- There is no evidence of staff training.
- Children are not aware of how to report a problem.



How do you ensure that all staff receive appropriate online safety training that is relevant and regularly up to date?







What mechanisms does the school, have in place to support young people and staff facing online safety issues?







How does the school educate and support parents and whole school community with online safety?







Do you have e safety policies and acceptable use policies in place? How do you know they are clear, understood and respected by all?







Describe how your school educates children and young people to build knowledge, skills and capability when it comes to online safety?

How do you assess it's effectiveness?







Media Use

	3 - 4	5 -7	8 – 11	12 - 15
Youtube	37%	54%	73%	87%
Social Media Profile	0%	3%	23% 21% to 43% (10-11)	72% 50% to 74% (12 -13)
Play online game with people they don't know			10%	21%
Chat in online games with people they don't know			5%	14%







Devices and Media Use

	3 - 4	5 -7	8 – 11	12 - 15
Internet via a PC/laptop/ netbook	24% (27%)	49% (56%)	66% (77%)	85% (82%)
Tablet Use	55% (53%)	67% (69%)	80% (70%)	74% (75%)
Access to Smartphone Ownership	23% 1%	28% 5%	57% 43%	91% 86%
Games Console	25%(34%)	52% (64%)	74%(77%)	67%(72%)

Ofcom 2016



What are our kids doing online?



Highlights from the Ofcom 2016 Report:

Tablet ownership

- 3-4's 16%
- 5-7's 32%
- 8-11's 49%
- 12-15's 49%

Phone ownership

Gaming devices

Boys vs Girls

- 3-4's 31% vs 19%
- 5-7's 66% vs 39%
- 8-11's 87% vs 60%
- 12-15's 85% vs 50%





What are our kids doing online?



Highlights from the Ofcom 2016 Report study:

Hours spent online

- 3 4's 14.12 hours a week
- 5-7's 12.24 hours a week
- 8-11's 13.30 hours
- 12 15's 14.42 hours

Social media profile

- 3 4 0%
- 5 7 3%
- 8-11's 23%
- 12-15's 72%

Online Gaming

- 3 4s 6.48 hours
- 5-7s 6.54 hours
- 8 11s 9.20 hours
- 12 15s 13.24 hours





Landscape 2012

*** BlackBerry





























Current Landscape















































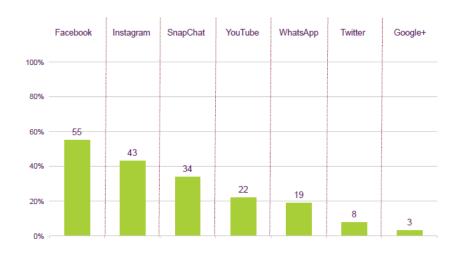
Social Networking – Where are we?











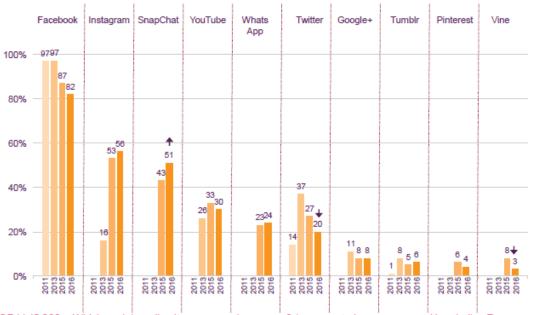






Social Media Use 12 – 15s

Figure 39: Social media sites or apps used by children aged 12-15: 2011, 2013, 2015 and 2016



QP44 /QC20 – Which social media sites or apps do you use? (unprompted responses, multi coded) – Responses from parents for 3-7 year olds and from children aged 8-15. showing responses of more than 2% of children aged 12-15 using any social media sites or apps. Base: Children aged 12-15 who have a social media profile (335). Significance testing shows any change between 2015 and 2016.

Both 8-11s and 12-15s are most likely to consider Facebook to be their main social media site







Can you name any sites children and young people use to:

- Game
- Social network
- Chat
- Share images

What devices would they use to access these sites?

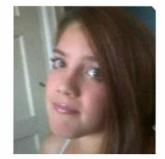
- Laptop/tablet
- Mobile
- Games consoles





Online Pornography









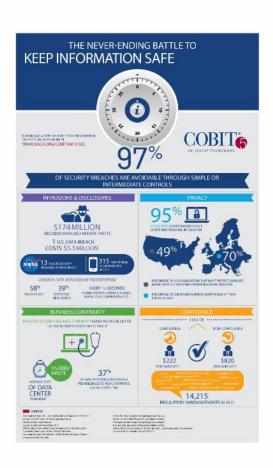








Privacy, Data and the Right to be Forgotten

















Mobile technology









Functionality of SmartPhones?

The ability to:

Browse the internet Take photos and film

Use location services Calendar

• Email Message

Take and share notes Telephone

WiFi





Risks Associated



Location Services

Access to unwanted internet sites

Text messaging

Social networking (including location aware apps)

The immediacy of photos





Online gaming



- Top 10 online game operators in Asia earned over \$2bn last year
- Web games:
 - World of War Craft
 - Runescape
 - Everquest
 - Swordsman Online
 - Mini Clip
- Games consoles (Xbox 360, Playstation 3, Wii)





Health Risks



- Repetitive strain injury
- Eye strain
- Obesity
- Addiction





Games Consoles



• There are controls on all the main games consoles









What is Cyberbullying?

How and where can you be Cyberbullied?

Cyberbullying





Cyberbullying is?



- Email
 - Forwarding comments
- Social networking sites
 - Profiles and adding comments
- Instant messenger and chat
- Mobile phones
 - Abusive texts
- Interactive gaming
 - On line chat
- Sending viruses
- Abusing personal information
 - Posting personal information









What does the 'inappropriate' mean in your house? Hampshire County Council



- Violence
- Racial Hate
- Pro eating disorders
- Gambling
- Pornographic







PEGI (The Pan-European Game Information age rating system) was established in 2003 to help European parents make informed choices



Vi

Violence - Game contains depictions of violence



Discrimination - Game contains depictions of, or material which may encourage, discrimination



Sex - Game depicts nudity and/or sexual behaviour or sexual references



Drugs - Game refers to or depicts the use of drugs



Fear - Game may be frightening or scary for young children



Bad Language - Game contains bad language







What is online grooming?

What does an online friend mean to your child? Is it the same for you?





Extremism



Police see extremism as:

- I. ISIS
- 2. Al Qaida
- 3. Irish Republican terrorism
- 4. Domestic Extremism / Extreme Right Wing
- 5. Animal Rights & eco-terrorism







Governors - What protection?

- Consider the age of the child when considering access to the Internet. What restrictions are necessary?
- Education and building awareness around inappropriate activity
- Staff training







Advice to parents

- Friends
 - School friends
 - Friends of friends
 - People who have an interesting profile
- Opportunities for people to be unkind





Stranger danger!!



Behaving on line only as you would behave in real life

Don't talk to people you don't know







Hampshire Services HIAS SCHOOL IMPROVEMENT

Setting Boundaries

- Set limits on the amount of time your child spends online set timings
- Make sure your child takes regular screen breaks
- Make sure your child thinks before they share pictures of videos online
- Make sure your child thinks carefully about what they write before they post it online
- Make sure your child doesn't give out personal details to people they don't know and trust
- Limit inappropriate and block illegal material
- Make sure your child knows to come to you if they are concerned about something
- Monitor activity
- Sometimes things go wrong Falling in the playground?







Is my child too young to have a Facebook account?

- Help set up their profile
- Add your email as the main contact (if possible)
- Set the privacy settings to "friends" only and ensure they are children you know
- Become a friend on Facebook
- Check in and keep updated









- 1. Only accept friends you know
- 2. Never share your password
- 3. Don't get personal
- 4. Use privacy settings
- 5. Don't react to bullies delete, block and report









- Use a strong password.
- Watch out for suspicious links, and always make sure you're on Twitter.com before you enter your login information.
- Use HTTPS for improved security.
- Don't give your username and password out to untrusted third-parties, especially those promising to get you followers or make you money.
- Make sure your computer and operating system is upto-date with the most recent patches, upgrades, and anti-virus software.



Generally



- Screen shot the abuse
- Changing the online name
- Never use a real name on a chat room
- Use an Avatar rather than a photo of
- Advise a child to tell an adult parent or teacher
- Don't retaliate
- Use the Report Abuse Button







Set controls on:

- Computers
- Laptops
- > Tablets
- Mobile devices
- Games Consoles
- > ALL internet enabled devices

that link to the <u>internet</u>

Set on all devices

Remember... they are not 100% accurate and not a substitute for open communication!









- I. Log in to your Google or Youtube account.
- 2. Go to the YouTube.com site in your web browser.
- 3. Click on the "Safety" button near the bottom of the YouTube homepage.
- 4. Click the "On" button. If you receive a message after clicking the on button that says "You can lock the Safety Mode setting after you sign in" then you are not logged into Google / YouTube. Click the "sign in" link if needed.
- 5. Check the box that says "Lock safety mode on this browser".
- 6. Click the "Save" button. After you've clicked the save button, the page you were on will reload and you will see a banner near the top of the page that shows a check mark with the words "Successfully enabled Safety Mode" next to it.
- 7. IMPORTANT!! In order to prevent your child from just turning safety mode off, you must log out of your Google / YouTube account by clicking your username link in the top right-hand corner of the browser window. This will effectively lock the setting in for the browser you are using, preventing your child from disabling Safety Mode. You will need to repeat this process for all other web browsers that are on your computer (i.e. Firefox, Safari, etc).

Enable YouTube Safety Mode on Your Mobile Device

Safety Mode may also be available on your mobile device's YouTube app. Check the settings area of the mobile app to see if it is an option. The process for locking the feature should be similar to the process above.

Setting Parental Controls on YouTube https://www.youtube.com/watch?v=u00yKwGFpS0







Controlling Content on a Smart TV

(I haven't managed to test this because I haven't got access to a SMART TV – I hope it works)

- Set up a You tube account on your computer (if you don't have an account)
- Once signed in, set your security features (see slide 22)
- Next open your Youtube app on your TV, and sign in.
- The TV should give you a code to associate your Youtube account with your TV.
- Go back to your computer and enter the code in your Youtube account (it should direct you to where this has to be done).

The only other way, would be blocking content for the whole TV using the Security settings from the TV's menu, which will block all content.





How to 'police' internet usage on handheld devices e.g. smartphones and How to set up mobile devices with limited content suitable for children



http://support.apple.com/en-gb/HT201304

IOS device restrictions

Apps for Android devices

MobileMinder (www.mobileminder.com)

Netaddictfree (http://netaddictfree.com/UK)

Qustodio (http://qustodio.com/









Tracks social media and texting

Some parent apps can actually monitor how fast someone is driving or moving in a vehicle as a passenger







Setting up restrictions on a router

http://kb.linksys.com/Linksys/GetArticle.aspx?docid=20 b29e54474a4a17aff594cb659747ea_4041.xml&pid=80& converted=0

This is a link for a Linksys router. Search 'restrictions on a ****** router'

Open DNS







Hampshire Services HIAS SCHOOL IMPROVEMENT

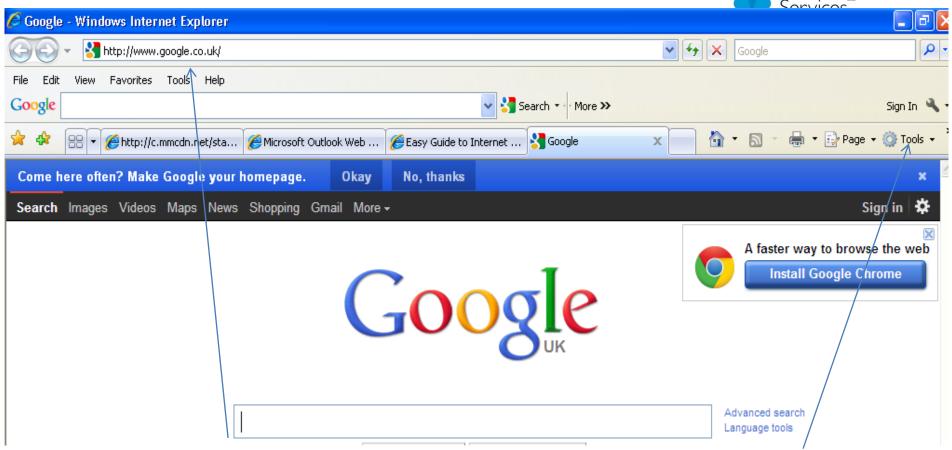
Parental Controls on the Internet

- Internet Explorer
- What about the router?



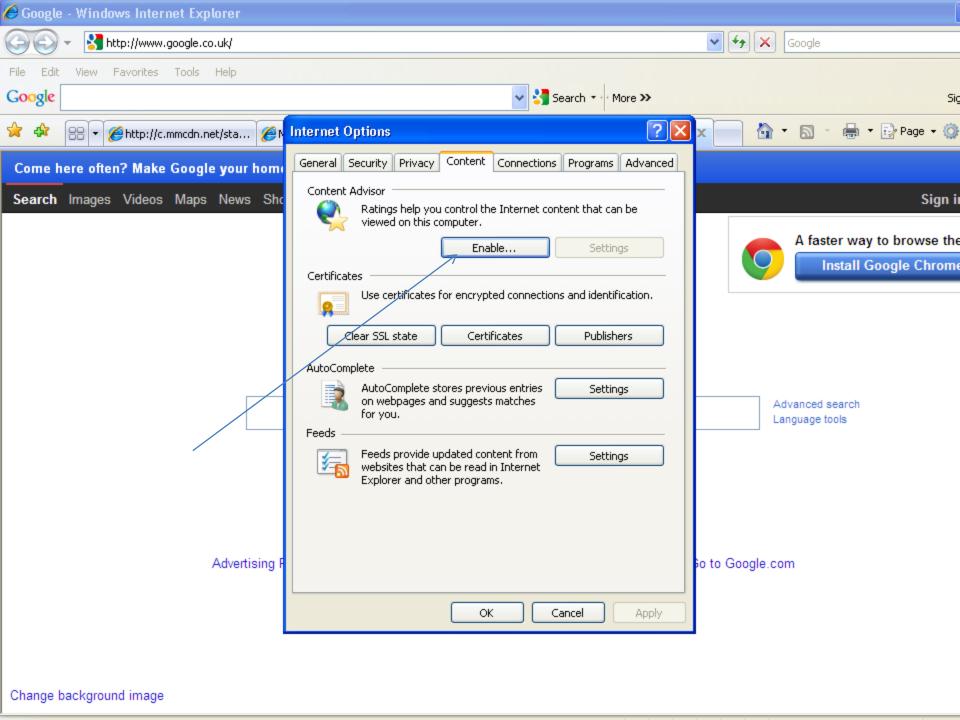


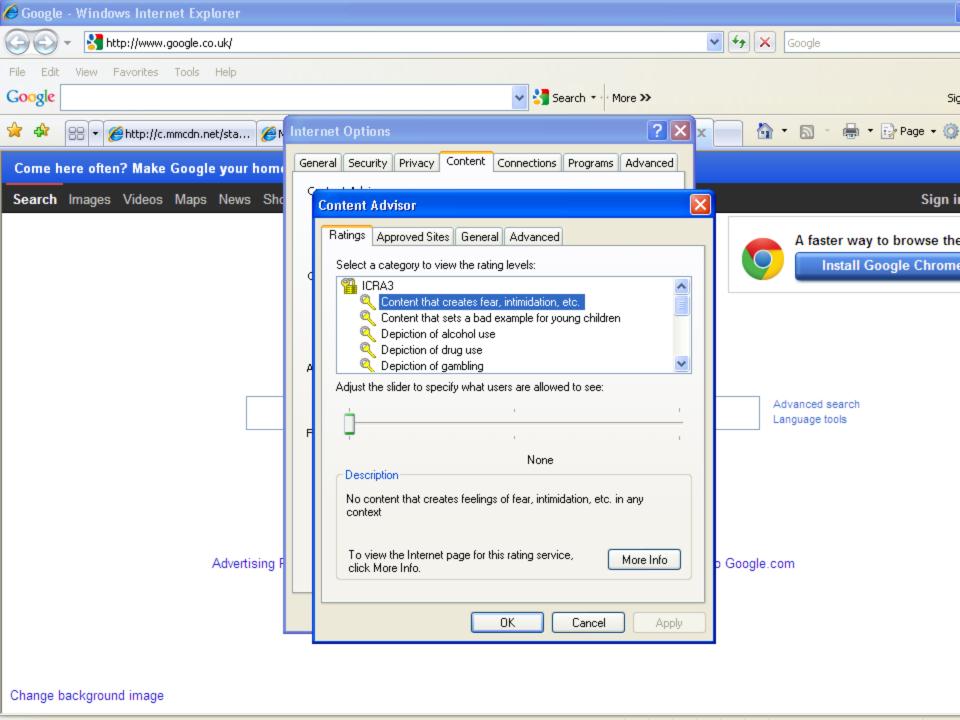












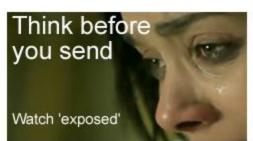


Welcome to CEOP's thin 11-16?

www.thinkuknow.co.uk/11_16/

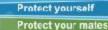
bsite





Come in to find the latest information on the sites you like to visit, mobiles and new technology. Find out what's good, what's not and what you can do about it. If you look after young people there's an area for you too - with resources you can use in the classroom, at home or just to get with it. Most importantly, there's also a place which anyone can use to report if they feel uncomfortable or worried about someone they are chatting to online. All the information here is brought to you by the team at the Child Exploitation and Online Protection (CEOP) Centre. We hope you like it!























Cyberbullying - Peer Mentoring



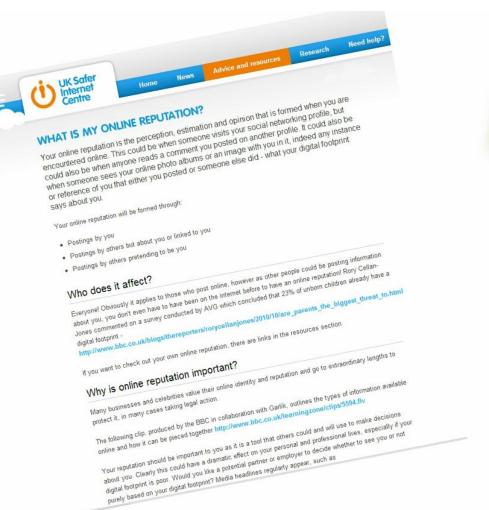
















www.saferinternet.org.uk/online-reputation









Home News Advice and resources Research N

A PARENTS' GUIDE TO TECHNOLOGY

In the parents' sessions we run in schools, we get a lot of questions about particular devices that children are using or asking for. This guide has been created to answer these questions and introduce some of the most popular devices, highlighting the safety tools available and empowering parents with the knowledge they need to support their children to use these technologies safely and responsibly.











View age appropriate animations and films at - <u>www.thinkuknow.co.uk/parents</u> <u>5-7</u> <u>www.youtube.com/ceop</u>



Lee and Kim's Adventure: Animal Magic

➤ Animation — Be nice to people, like you would in the playground

Jigsaw

Safe Social Networking Hampshire
County Council



8-10

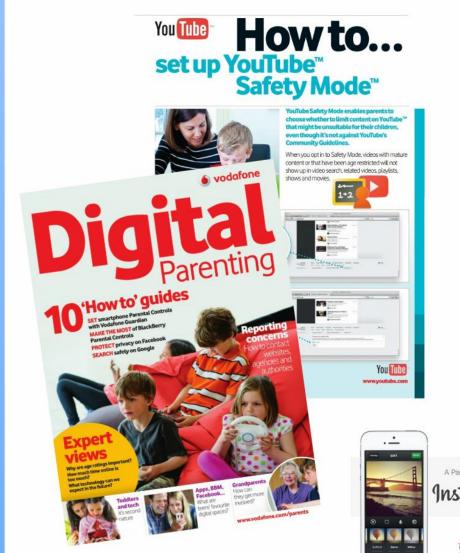


Resources



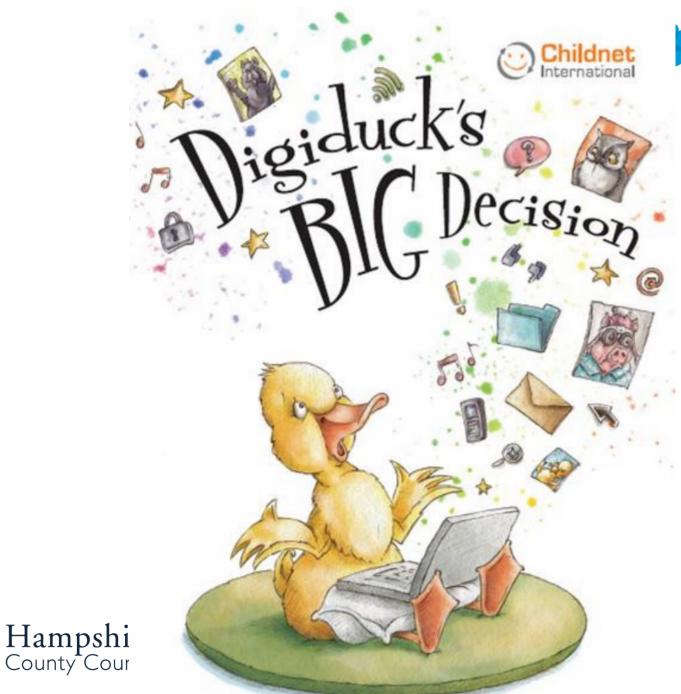








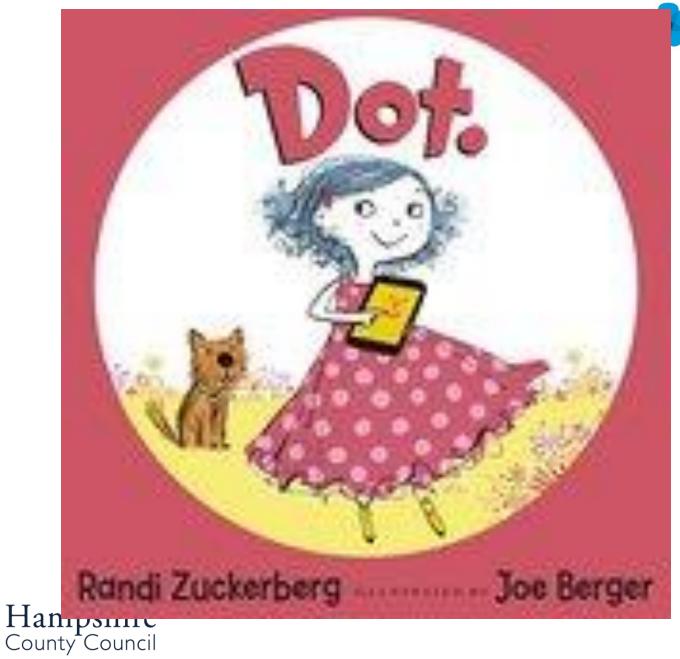






HIAS SCHOOL IMPROVEMENT





Hampshire Services

HIAS SCHOOL IMPROVEMENT







HANNAH WHALEY



HIAS SCHOOL IMPROVEMENT





Monitoring another mobile phone

There are a number of Apps that will do this. There is a cost associated with all the ones that I found that carry out comprehensive tracking.

Phonesheriff is a recent App that tracks all phone activity on another phone

The link for this is:

http://www.phonesheriff.com/features.html













- Security
- Policies
- Websites
- Photographs

Report on the data protection guidance we gave schools in 2012











Zero to Eight

Young children and their internet use

August 2013







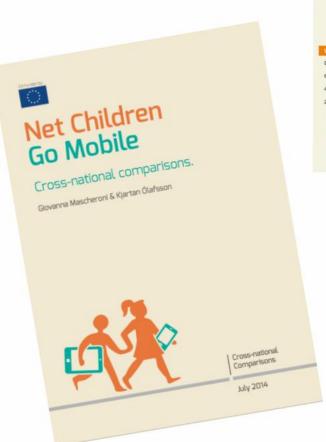


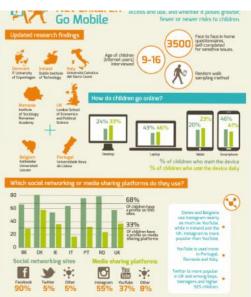


Donell Holloway, Lelia Green and Sonia Livingstone with members of the *EU Kids Online* network

ISSN 2045-256X

www.eukidsonline.net











Counter Terrorism and Security Act 2015

Obliges schools to...

- Assess the risk
- Be prepared
- Work in partnership
- Train your staff
- Educate your students
- Implement strict IT policies
- Take responsibility







Education Act

PART 2DISCIPLINE2 Power of members of saff at schools to search pupils(1) Chapter 2 of Part 10 of EA 1996 (punishment and restraint of pupils) isamended as set out in subsections (2) to (5).(2) In section 550ZA (power of members of staff to search pupils for prohibiteditems: England)—(a) in subsection (3) (prohibited items), after paragraph (e) insert—"(ea) an article that the member of staff reasonably suspectshas been, or is likely to be, used—(i) to commit an offence, or(ii) to cause personal injury to, or damage to theproperty of, any person (including P);";Power of search - reasonable force(b) in that subsection, after paragraph (f) insert—"(g) any other item which the school rules identify as an itemfor which a search may be made.";Current search for banned items is by consent but school may apply discipline procedures if that consent is not given. New law when enacted requires no co







The person who seized the item may examine any data or files on the device, if the person thinks there is a good reason to do so.

(6F) Following an examination under subsection (6E), if the person has decided to return the item to its owner, retain it or dispose of it, the person may erase any data or files from the device if the person thinks there is a good reason to do so.









degree safe









the online e-safety tool





Policies and Guidance Documents

Schools should consider whether they have:

- Online safety policies should include references to
 - Social media
 - Use of mobile phones and personal devices
 - Use of images and cameras
 - Training pupils and staff

These should have been developed in consultation with all stakeholders and reviewed on an annual basis

- An acceptable use policy for all staff and pupils
- A nominated online safety lead
- An understanding of the implications of the data protection act in the context of online safety
- A secure network where devices leaving the site are encrypted and strong passwords are used.
- An accredited education supplier for the Internet where there is an appropriate internet service provider and relevant filtering and monitoring products.
- Online safety training for all school staff with a comprehensive online safety curriculum delivered to all pupils



What next?



Sue.savory@hants.gov.uk



