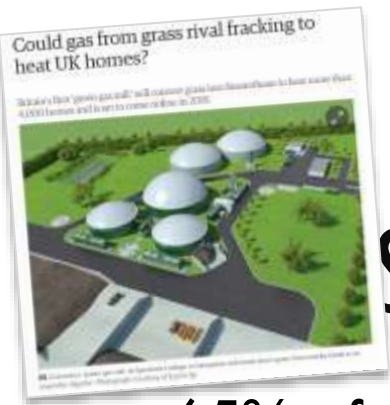


ONLINE SAFETY

Practical parenting
in the digital age

Derek Crabtree – London Borough of Merton derek.crabtree@merton.gov.uk



SHAPE OF THINGS TO COME

65% of children will end up at jobs that haven't been invented yet

Alternative Currency Bankers

3D Printing Engineers

Waste Data Managers

Urban Agriculturalist

Nano-Medics / Robotic engineers

Anaerobic digester architect

Drone Dispatchers / Pilots

YouTuber

Certified Ethical Hacker



Samsung's Family Hub 2.0, has internal cameras, voice control and an interface to the MasterCard Groceries app for easy ordering. It knows what people are eating more surely than any supermarket.



INTERNET OF THINGS

Computer

Tablets

Laptops

Smart

Televisions SMART

Games Consoles

Hand held
games consoles

ers



Cameras – Geo tagging

Wearables – Fit Bit

DVD/Blu Ray Player (Netflix)

Burglar Alarm

Car

Heating System

Fridge

Toys – Hello Barbie

Baby Monitors

SMART Meds

More connected devices mean more attack surfaces and greater risks and more possibilities for hackers.



DDOS

A golden retriever is shown in profile, facing right, with its mouth open and tongue out, appearing happy. It is wearing a brown leather collar with a metal buckle and a black leash. The dog is standing in a lush green field with some yellow wildflowers. To the left, the lower leg and blue jeans of a person are visible, holding the leash. The background is a soft-focus green field.

Pooper

Your dog's poop in someone else's hands.



SEE HOW IT WORKS

WHEN IS A TOOTHBRUSH NOT A TOOTHBRUSH?



I AGREE

facebook

Connect with friends and the world around you on Facebook.



See photos and updates from friends in News Feed.



Share what's new in your life on your Timeline.



Find more of what you're looking for with Graph Search.

By clicking Sign Up, you agree to our Terms and Conditions, read our Data Use Policy, including our Cookie Policy, and our Privacy Policy.



WHAT ARE YOU AGREEING TO?

When we click “I agree,” we hand over the right to

- Track us
- Profile us
- Scan our email
- Scan chat content;
- Remove, edit, or share and sell our content without giving us a cut of the revenues.



How long for?

Facebook “likes” alone can reveal an individual’s gender, age, race, sexuality, political, and religious views.

Target correctly inferred that a teenage girl was pregnant based on big data profiling—as her father found out when he phoned to complain that she’d been sent coupons for baby products.

THE WORLD'S MOST VALUABLE RESOURCE IS NO LONGER OIL, BUT DATA

A NEW commodity spawns a lucrative, fast-growing industry, prompting antitrust regulators to step in to restrain those who control its flow.

A century ago, the resource in question was oil. Now similar concerns are being raised by the giants that deal in data, the oil of the digital era.

Amazon captures half of all dollars spent online in America. Google and Facebook accounted for almost all the revenue growth in digital advertising in America last year.



What has changed?

Smartphones and the internet have made data abundant, ubiquitous and far more valuable. Whether you are going for a run, watching TV or even just sitting in traffic, virtually every activity creates a digital trace—more raw material for the data distilleries

HOW TO STAY PROTECTED AGAINST RANSOMWARE

Updates – always update, devices and apps

Anti-Virus – keep up to date

Anti-Malware – Keep up to date

Get Savvy – Educate yourself and don't fall prey

Backup your data – make use of cloud services

Unplug USB drives when not in use

PUPIL PREMIUM ELIGIBILITY

Free Anti Virus

The 'Pupil Premium / Free School Meals Service' www.fsm.lgfl.net is a web site where parents can quickly and easily check eligibility for free school meals and, if eligible, also gain welcome additional funding for their child's school, known as 'Pupil Premium'. If eligible, you are not obliged to accept the free school meals for your child if you wish to make other arrangements, but we do want to encourage applications as the additional funding gained would still benefit education provision at the school.

By way of a 'thank you' to parents for taking part, and regardless of individual outcomes, The London Grid for Learning (LGfL) would like to provide parents of children attending LGfL-connected schools with **Sophos Anti-Virus software, free of charge**, to protect the computers used by pupils at home.

To gain access to this software there is a short registration process which will also give you access to other LGfL services and benefits that are available to your child's school. Please be assured there is no catch, no cost and no advertising. LGfL (a UK education charity set up in 2001 and owned by London's 33 local authorities) exists to support education and is leading this initiative to make it easier for parents to apply for free school meals and to encourage the drawdown of unclaimed Pupil Premium.

Please visit www.fsm.lgfl.net enter the necessary details and support this worthwhile initiative.

PROTECTING YOUR PHONE

- Get software that allows you to lock, locate, and wipe your device
- Always use a PIN or password to lock phone
- Only download apps from trusted stores
- Back up data
- Keep OS and apps updated
- Log out of sites after you make a payment
- Turn off Wi-Fi and Bluetooth when not in use
- Avoid giving out personal information



THE DARK NET



Home

Anonymity Online

Protect your privacy. Defend yourself against network surveillance and traffic analysis.



Download Tor

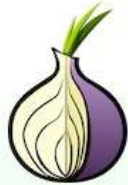
About Tor - Tor Browser

About Tor

Tor Browser | Search or enter address

The green onion menu now has a security slider which lets you adjust your security level. Check it out! [Open security settings](#)

Tor Browser 6.0.4



Welcome to Tor Browser

You are now free to browse the Internet anonymously.

[Test Tor Network Settings](#)

Search securely with Disconnect.me.

What Next?

Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

[Tips On Staying Anonymous »](#)

You Can Help!

There are many ways you can help make the Tor Network faster and stronger:

- [Run a Tor Relay Node »](#)
- [Volunteer Your Services »](#)
- [Make a Donation »](#)

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. [Learn more about The Tor Project »](#)

TEENAGE CYBERCRIME NATIONAL CRIME AGENCY



<https://www.youtube.com/watch?v=DjYrxzSe3DU>

CHANGED TIMES



Children growing up now have never known a time without the internet.

Children aged five to 16 spend an average of six and a half hours a day in front of a screen compared with around three hours in 1995, according to Childwise.

THE CHALLENGE

1. Children and young people make up one-third of internet users
2. They see little distinction between offline and online.
3. They test relationships, experiment and push boundaries, constantly asking themselves questions about the person they want to be
- 4.the internet is vital for satisfying this curiosity
5. They should be encouraged to learn, explore and interact with one another online, but the content they can access, and the online space that they are navigating, must be age-appropriate and safe.

GROWING UP DIGITAL

January 2017

The report, which the Government said it would now look at “carefully”, calls for:

- an end to “impenetrable terms and conditions” that “give social media giants control over children’s data without any accountability”.
- a digital ombudsman to help children to remove content about themselves and force firms to be more transparent
- a compulsory digital citizenship programme in every school from ages 4-14

Government launches major new drive on internet safety

01 March 2017

This week the Government has announced that Ministers have begun work on a new Internet Safety Strategy aimed at making Britain the safest country in the world for children and young people to be online.

Culture Secretary Karen Bradley is leading the new cross-Government drive on behalf of the Prime Minister – with a green paper expected in the summer.

A report by leading academic Professor Sonia Livingstone has been commissioned to provide up to date evidence of how young people are using the internet, the dangers they face, and the gaps that exist in keeping them safe.

Ministers will also hold a series of round tables in the coming weeks with social media companies, technology firms, young people, charities and mental health experts to examine online risks and how to tackle them.

The work is expected to centre on four main priorities: how to help young people help themselves; helping parents face up the dangers and discuss them with children; industry's responsibilities to society; and how technology can help provide solutions.

The focus will be on preventing children and young people from harm online and making the internet a safer place.

At the UK Safer Internet Centre we look forward to contributing to this strategy which will help strengthen the ongoing work taking place across the UK to empower children and young people to use technology safely, responsibly and creatively.

WHAT IS THE
INTERNET?

What is the internet ?

SCREEN TIME

'Screen time' is an obsolete concept. As digital media become integrated aspects of daily life, the concept of 'screen time' is obsolete.

Parents could consider whether children are:

- Eating and sleeping enough
- Physically healthy
- Connecting socially with friends and family – through technology or otherwise
- Engaged and achieving in school
- Enjoying and pursuing hobbies and interests – through technology or beyond
- Having fun and learning in their use of digital media?

If the answer to these questions is more or less 'yes', then perhaps the problem of 'screen time' is less dramatic than many parents have been led to believe.

USING SCREEN MEDIA WITH YOUNG CHILDREN

Research shows that children's learning from media can be greatly enhanced when parents and other adults join in and make it a shared experience. The following tips offer a range of ways you can use screen media to make it an interactive, more enriching learning experience.

- Watch Together
- Play Screen-Based Games Together
- Make the Connection Between the Screen and the Real World

NEVER TALK TO STRANGERS

building resilience...

It would be more helpful if we were to look at ways in which we can help young people recognise when grooming takes place and how to identify strategies to stay safe.

“Never talk to strangers” isn’t helpful advice – each of us speaks with strangers every day.

We need to provide our young people with the skills and strategies to stay safe while engaging with strangers, who may be, or appear to be, online friends.

THE REAL WORLD

*A child is a child
until they reach
maturity, not until
they pick up a
smartphone*

Too often adults will make a distinction between the 'real' and 'online' world.

Understand that the online world is the real world. - Social media is about people.

The challenges our children face online are about **people and relationships**, not buttons and technology.



RISK VS HARM

Risk - the possibility that something negative or dangerous will happen

Harm - refers to actual damage or trauma

There are certainly risks associated with internet use, but for the majority of young people, **these risks will never lead to harm.**

E-SAFETY

**‘A parent who can help their child
navigate the offline world will help
them navigate the online world’**

Dr Pooky Knightsmith

“Its about transferring your off line parenting skills online”



WHAT KIND OF PARENT WILL YOU BE?

Enablers “They’ve given in to their kids’ expertise and allow them to set the family’s tech agenda.” (Teenagers parents)

Digital limiters, “Heeding widespread concerns about the impact of technology use on children’s attention spans and interpersonal relationships, limiters take every opportunity to switch off screens.”

Digital mentors take an active role in guiding their kids onto the Internet. “Mentors, in fact, may be the parents who are most successful in preparing their kids for a world filled with screens, working actively to shape their kids’ online skills and experiences.”

ALEXANDRA SAMUEL

ONLINE PARENTING

“Children of **limiters** are most likely to engage in problematic behaviour:

twice as likely as the children of **mentors** to access porn, or to post rude or hostile comments online;

three times as likely to go online and impersonate a classmate, peer, or adult.”

“Shielding kids from the Internet may work for a time, but once they do get online, limiters’ kids often lack the skills and habits that make for consistent, safe, and successful online interactions.”

ALEXANDRA SAMUEL

CHILDREN'S DATA - SHARENTING



For many children online life begins before birth, when their excited parents-to-be post ultrasound images on social media.

The average parent will share their child's image online nearly 1500 times before their fifth birthday.

Once information about your children is on the internet it can be difficult for them to control it and so we need to be considerate when we share things on their behalf.

Respecting this right to a private life now, and in the future, and involving them in decisions about what to post online once they are old enough, is not only good manners, it could also help them learn the importance of thinking before they share things on social media themselves.



Safety Centre

Policies
Tools
Resources

Bullying Prevention Hub

Teens
Parents
Educators

Parents Portal

Get to know Facebook
Parenting tips
Expert advice

Help Centre

Security Check-up
Privacy Check-up
Suicide hotlines

Safety@Facebook

People come to Facebook to share their stories, see the world through the eyes of others and connect with friends and family. Our mission is to give people the power to share and to make the world more open and connected. We want everyone to feel safe when using Facebook.

We work with external experts, including a Safety Advisory Board, and gather feedback from our community to develop policies, tools and resources to keep you safe.

Before you share, ask yourself:

- Could somebody use this to hurt me?
- Would I be upset if someone shared this with others?
- What's the worst thing that could happen if I shared this?

Always remember that the things you share with your friends can end up being shared with others.

Friending

- Following
- Unfollowing
- Unfriending
- Blocking

Reporting

Community Standards.

Facebook includes a link in nearly every piece of content for reporting abuse, bullying, harassment and other issues.

DATA TO GO



HELPFUL CHECKS

Who's looking?

- When did you last check your privacy settings?
- Google your child's name to review the information you post
- Remember that anyone who can see a photo can also download or screenshot it, and could go on to share it.

What else are you sharing?

- As default, many cameras, phones and apps tag posts and photos with 'meta-data' which can include location details and other identifying information

Ownership

- Under the terms and conditions of most social networks, when you share a photo you license the network to use and reproduce your image, and grant it the right to license it for use by third parties.

Your child's digital tattoo

- Every publically accessible image or comment featuring your child contributes to a public image which will follow them into the future.

FOR YOUNGER CHILDREN



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.

FOR OLDER CHILDREN

stay safe online

Remember the 5 SMART rules when using the Internet and mobile phones.



S

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.



m

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.

a

ACCEPTING: Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!



r

RELIABLE: Someone online might lie about who they are, and information on the internet may not be true. Always check information with other websites, books or someone who knows.



t

TELL: Tell your 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.



Find out more at Childnet's website ...

www.kidsmart.org.uk

Childnet International © 2002-2010 Registered Charity no. 1080173 www.childnet.com



THE RISKS

content: being exposed to illegal, inappropriate or harmful material;

contact: being subjected to harmful online interaction with other users; and

conduct: personal online behaviour that increases the likelihood of, or causes, harm.

CRITICAL THINKING ONLINE: A PARENT'S GUIDE

It's hard enough for adults to recognise advertising and resist ridiculous rumours online, but it can be even more complicated for young people.

Advertising

Have you ever looked at a spread in a magazine, only to realise all the clothes are from the same brand and the feature is actually an advertisement?



Rumours

Misunderstandings and misinformation can spread quickly online, so it's important to remember that just because something is trending doesn't mean it's true. #nowthatchersdead

Clickbait

With so many media outlets online there's a lot of competition for clicks and attention, and it can be tempting to exaggerate to get someone to click on your story.

Some examples of clickbait are laughably obvious – any headline ending in 'you won't believe what happened next,

CRITICAL THINKING

What's real? What's fake? What's satire?

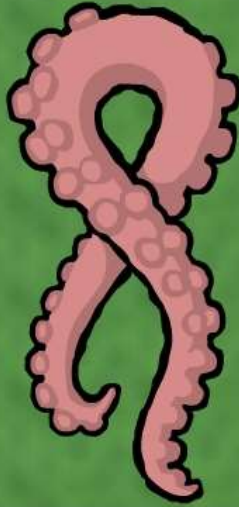
Here are a few basic questions to consider whenever you and your kids encounter a piece of media:

- Who made this?
- Who is the target audience?
- Who paid for this? Or, who gets paid if you click on this?
- Who might benefit or be harmed by this message?
- What is left out of this message that might be important?
- Is this credible (and what makes you think that)?

FAKE NEWS

Drop bear

Australian Geographic ran an article on its website on 1 April 2013 (April Fools' Day) purporting that researchers had found that drop bears were more likely to attack tourists than people with Australian accents



CEPHALONEWS

2016-09-01 Cuttlefish Can Count To Five (Inkfish | Discover)

Don't look now, but *Sepia pharaonis* cuttlefish may be able to count better than your toddler.

2016-08-23 Shy Octopus Hides Inside Its Own Tentacles (EViNautilus)

(Video) While diving off the central California coast, the team of E/V Nautilus encountered this Flapjack Octopus (named for its ear flaps) lingering on the sea floor. **Another video.**

2016-08-20 'Googly-Eyed' Stubby Squid Captures Internet's Attention (NPR)

It looks like it could be a cartoon character, but it's real. And this little squid is making waves on the internet.

» Older news...

CEPHALOBLOG

Help Save The **ENDANGERED** PACIFIC NORTHWEST TREE OCTOPUS From **EXTINCTION!**

[About](#)[HELP!](#)[FAQs](#)[Sightings](#)[Media](#)[Activities](#)[Links](#)

THE PACIFIC NORTHWEST TREE OCTOPUS

The Pacific Northwest tree octopus (*Octopus paxarbolis*) can be found in the temperate rainforests of the Olympic Peninsula on the west coast of North America. Their habitat lies on the Eastern side of the Olympic mountain range, adjacent to Hood Canal. These solitary cephalopods reach an average size (measured from arm-tip to mantle-tip,) of 30-33 cm. Unlike most other cephalopods, tree octopuses are amphibious, spending only their early life and the period of their mating season in their ancestral aquatic environment. Because of the moistness of the rainforests and specialized skin adaptations, they are able to keep from becoming desiccated for prolonged periods of time, but given the chance they would prefer resting in pooled water.



Rare photo of the elusive tree octopus

An intelligent and inquisitive being (it has the largest brain-to-body ratio for any mollusk), the tree octopus explores its arboreal world by both touch and sight. Adaptations its ancestors originally evolved in the three dimensional environment of the sea have been put to good use in the spatially complex maze of the coniferous Olympic rainforests. The challenges and richness of this environment (and the intimate way in which it interacts with it,) may account for the tree octopus's advanced behavioral development. (Some evolutionary theorists suppose that "arboreal adaptation" is what laid the groundwork in primates for the evolution of the human mind.)

Reaching out with one of her eight arms, each covered in sensitive suckers, a tree octopus might grab a branch to pull herself along in a form of locomotion called tentaculation; or she might be preparing to strike at an insect or small vertebrate, such as a frog or rodent, or steal an egg from a bird's nest; or she might even be examining some object that caught her fancy, instinctively desiring to manipulate it with her dexterous limbs (really deserving the title "sensory organs" more than mere "limbs",) in order to better know it.

Tree octopuses have eyesight comparable to humans. Besides allowing them to see their prey and environment, it helps them in inter-octopus relations. Although they are not social animals like us, they display to one-another their emotions through their ability to change the color of their skin: red indicates anger, white fear, while they normally maintain a



REAL OR FAKE PHOTO

Play this game with your kids : <http://www.fakeaphoto.com/real-or-fake-photo-game/>

SOCIAL MEDIA CONTACT



“Before the internet, someone with a sexual interest in children had to take lots of risks,”



“They needed to loiter near schools, go to the beach or park.



“Now, they can browse huge amounts of content from the privacy of their own homes, and no one knows they have done it.”

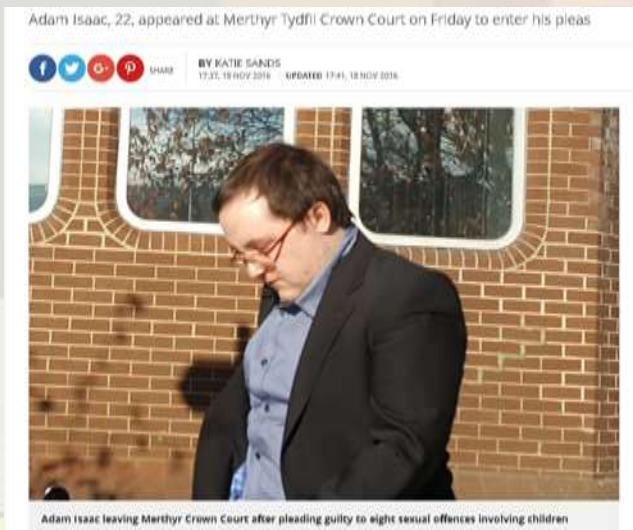
Karl Hopwood, UK Council for Child Internet Safety.

THE CASE OF JOEL



Joel was one of **two victims** of Adam Isaac, who used Minecraft to lure his victim onto other platforms – including **Skype** and **Snapchat** – to groom them.

Joel's Dad, Lee, revealed how Isaac had built up a strong friendship with his son Joel (also not his real name), won his trust and sent him money through **PayPal** before turning the conversation towards pornography.



Joel was part of a **'faction'** on Minecraft - a group that plays together online in order to protect their bases and raid others.

Players are able to have limited communication in the game, so in order to plan secret 'attacks' on other factions they move onto other chat services like **Skype**.

The background of the slide features a faint, grayscale image of a person's head and shoulders in profile, wearing a large, over-ear headset with a microphone. The person's face is obscured by a solid gray silhouette. The headset has a flexible boom arm and a circular microphone at the end. The overall tone is somber and investigative.

THE CASE OF JOEL

“We never let him have a camera so everything was done by audio. We always knew who he was talking to, we would talk to them as well because we’d come in his room to check. It would be some kid from Australia or somewhere and they’d ask how your dad is and so on.” Joel’s Dad (Lee)

Lee noticed a change when Joel started using headphones when on Skype

THE CASE OF JOEL

As Isaac conducted much of the abuse over video, there was little trace of the exchanges.

“Fortunately Joel never met him in person. But Isaac made him watch things on camera, he would send Joel pictures of himself. He sent him links to pornography, saying ‘watch this’.”

“And 12-year-olds are curious.”

Lee managed to identify Isaac via the payments the groomer made to Joel over PayPal, as in one payment there was reference to his name and address.

He went straight to the police.



THE CASE OF

A man who groomed young boys through the online game Minecraft has been jailed for two years and eight months. 20th January 2017

Adam Isaac, 22, of Merthyr Tydfil , appeared at Merthyr Tydfil Crown Court on Friday to enter his pleas.

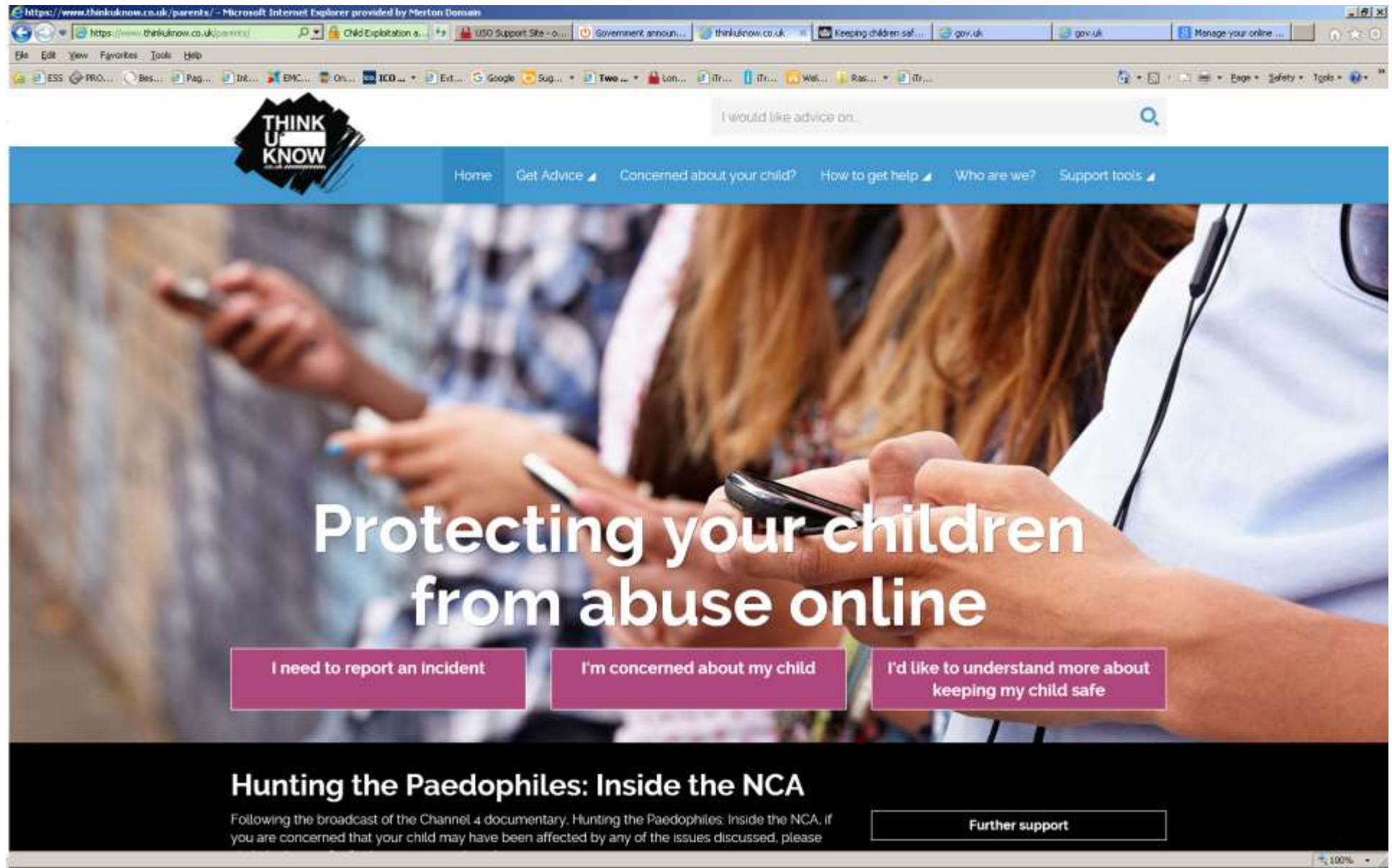
Isaac admitted

- two counts of causing or inciting child prostitution or pornography,
- one count of engaging in sexual activity in the presence of a child, and
- causing or inciting a child to engage in sexual activity
- three counts of causing or inciting child prostitution or pornography
- Isaac also pleaded guilty to possessing indecent images of children.



"This case serves as another reminder to anyone who has caring responsibilities for children to be alert to online safety matters so that wherever possible, children are prevented from coming into harm's way."





<https://www.thinkuknow.co.uk/parents>

TIPS AND ADVICE FOR PARENTS AND CARERS

1. Be engaged

Talk regularly with your children about how they use technology, and find out what their digital life is like, including how they communicate using images and videos. Perhaps you can start off by discussing your favourite emojis?



2. Be aware

Explore the online features of the devices you already own in your family and the devices you might buy for your child in the future.

Knowing how to activate and use parental controls can help protect your child from seeing inappropriate content online.

For advice and guides on how to make use of parental controls and other safety features on devices, check out [Parents' Guide to Technology](#).

3. Be there

The most important thing is to ensure that you are there if something goes wrong. Your child might be very embarrassed to discuss the issue they are facing so reassure them that they can turn to you no matter what.

You are always there to help your children but make sure you know how to get support too by visiting the [‘Need Help?’ page](#).

4. Be thoughtful

The internet provides a platform for billions of people to share their views and opinions but not everything or everyone online is trustworthy.

Encourage your children to **think critically** about the things they see - help them consider the difference between fact and opinion, and that there is sometimes more than meets the eye.

Need some help starting a conversation? [conversation starters for ways of striking up a conversation with your child about what they see online](#).

MINECRAFT:

A PARENT'S GUIDE

SINGLE PLAYER VS MULTIPLAYER

Single player

Safest mode.

Users play by themselves and can't use the chat function to communicate with anyone else.

Might be more appropriate for very young children.

Multiplayer

Server-based version that lets multiple users play together in a single world.

Players can communicate using the chat function – press T and then Enter to display the chat to others.

Has some risks but can still be used safely.

STAYING SAFE ON MINECRAFT

Turn off chat

Find a child-friendly server

Set time limits

Talk to them

You could also ask them to show you their Minecraft world.

As with any online activity, there are some safety concerns to keep in mind.

- Set the account up through **your own email address** and know their passwords – at primary age, this is not an unreasonable thing to ask.
- **Discuss** which settings you are going to apply prior to their joining the site – will you allow multiplayer, for instance?
- Speak to your child about **unwanted contact** and **what to do** if someone is being nasty or inappropriate to them in the game. Ask that they come to you if anything goes wrong, so you can make it stop.

MINECRAFT



Our Family's Official Minecraft Constitution



We, the undersigned, agree to abide by the following rules of Minecraft while living in our parents' house:

1. No stealing from friends or family members' chests.
2. No killing friends or siblings in Minecraft.
3. No trapping unless you are in a designated trapping world. And if you get trapped and accidentally killed in a designated trapping world, no crying about it.

If You Break the Rules of Minecraft in our House:

The punishment is a minimum of 168 hours of Minecraft Banishment. (That's 7 days, folks!)

Anyone who accidentally kills somebody can request a special court hearing to make a formal appeal. The ruling of the judge on duty is final (whether it is a babysitter, mom, dad, or any other adult in charge). If you are found guilty after an appeal the punishment will be a minimum of 168 hours plus an additional 48 hours for your dishonesty. (That's 9 days!) So don't appeal unless you think you can win it.

You **MUST** sign your name in the box below to PLAY:



SSSSSSSS....

Happy Crafting, Folks!



© healthy-family.org

FAMILY AGREEMENT

http://www.childnet.com/safety-leaflets-for-parent:2016?utm_content=bufferial&utm_source=twitter.co

Things to consider...

Keeping safe

- How safe is our personal information?
 - Do we have strong passwords? Eg capital letters, symbols etc
 - Do we all have usernames that don't reveal our full names?
- Have we considered parental controls which would be right for our family?
- Have we discussed online friendships and whether we can trust them?
- Do we need a family email address?
- Who will we talk to if we feel uncomfortable about anything we have seen or heard online or on a mobile phone or gaming device?
- When is it okay to download files, games or apps?
- Have we checked the reviews and ratings for apps and games?
- Which websites are okay for us to use?
- Should we open links from people we don't know?

Social networking

- Do we know the age requirements to be on social networks?
- Who can I post photos of online?
- Do I know why it is important for my accounts to be private?

Gaming

- Which age rated games can I play?
- Am I aware of why PEGI is important?
- Can I play online with people I don't know?

Positive online behaviour

- How can I be a good friend on the internet?
- What will I do if I receive frightening or bullying messages?

Healthy lifestyle

- How long can we spend online?
- Do we spend the same amount of time enjoying our offline activities?
- Where can we use our devices around the house?

Examples

Suggested ideas for an agreement with younger children.

We agree to...

I will use my tablet for _____ mins a day

We will make sure the children's favourite games are bookmarked for them to get to easily

Who is responsible for this?

Isabel and Phoebe

Mum and dad

Suggested ideas for an agreement with pre-teen children.

We agree to...

I will tell mum and dad when I see something that worries me

We will put parental controls in place but review it as the children grow up

Who is responsible for this?

Jack and Tom

Mum and dad

Suggested ideas for an agreement with teenage children.

We agree to...

I will make sure all my social networking sites are private and that I only accept requests from people I know

We won't post photos of our children without their permission

Who is responsible for this?

Jane, John and Ben

Mum and dad

the smart talk

Put your internet rules in writing!

<https://thesmarttalk.org/#/>

The Smart Talk gets parents and kids together for a conversation about being responsible with new technology.



1

Have your kid join you. Making decisions together gets everyone on the same page.



2

Answer a series of questions. These will set a few ground rules for all your devices.







3

Print your very own agreement. Then post it where the whole family can see, like on the fridge.

PUTTING THE **FAMILY AGREEMENT** INTO PRACTICE

A family agreement is a great way to start a conversation with your whole family about how you all use the internet and discuss together how to behave in a positive way when online at home, at school or at a friend's house.

-  Make sure that both adults and young people are open to changing their online behaviour as a result of your agreement.
-  Make sure your agreement works for your whole family and everyone is happy with it.
-  Review your agreement in the future to make sure it reflects the current needs and ages of your family.
-  Consider your tone - Are you focusing on negative behaviour or promoting positive behaviour?

GAMING APPS



- no age verification
- no reporting facilities within Clan chat

If your child is going to use the multi-player option of the game unsupervised, be aware that they may come across adults and bad language - occasionally even both at the same time.

The game was the top grossing app on both the App Store and Google Play, with an estimated revenue of over £1 million (1.5million dollars) per day.

Gabriel is 11 and plays with his parents' permission. He says: 'I like how it's almost never ending and I can play with my friends on it.'

'I'm in one clan with friends from school. I don't really chat on it because I don't want other people seeing my info so we talk on Skype or ooVoo when we're playing. The bad thing is that it takes a long time to progress and you have to wait a day for some things, which is annoying.'

'It's OK for little kids like my cousin (6), to play under supervision and their new game, Clash Royale, is good, maybe even better!'

POINTS
1,109,400
TIME
09:55
MISSIONS

IN APP PURCHASES



George Holmer of Nottinghamshire was appalled to find his 11-year-old son had forked out £3,500 to buy “gold” in a game called Arcane Empires, a “free” app.

Doug Crossan from Bristol discovered that his 13-year-old son had spent £3,700 on 300 purchases made in games such as Hungry Shark and Gun Builder (both “free” games) and Plants v Zombies (69 pence to download). Mr Crossan is a police officer. He reported his son to the police, in effect for fraud.

Mr Crossan said: “I am a father of a studious, polite and sensible 13-year-old who has been duped after uploading free children’s games on his iPod and iPad.”



iOS

The restrictions menu in iOS allows you to require a password for every purchase made on your iOS device.



1. Tap Settings -> General -> Restrictions



2. Tap Enable Restrictions

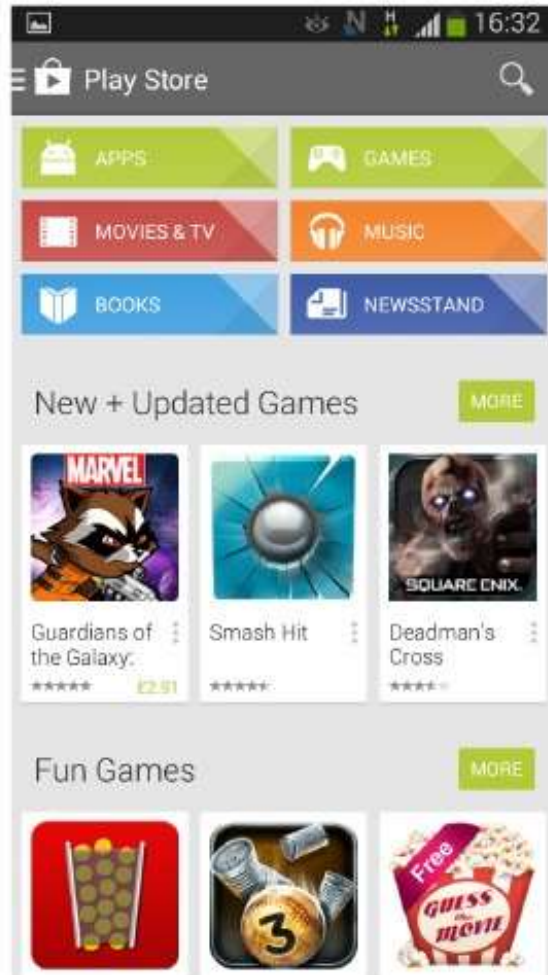


3. Choose a restrictions passcode that you will remember and confirm your passcode. We recommend choosing a passcode different from the passcode you use to unlock

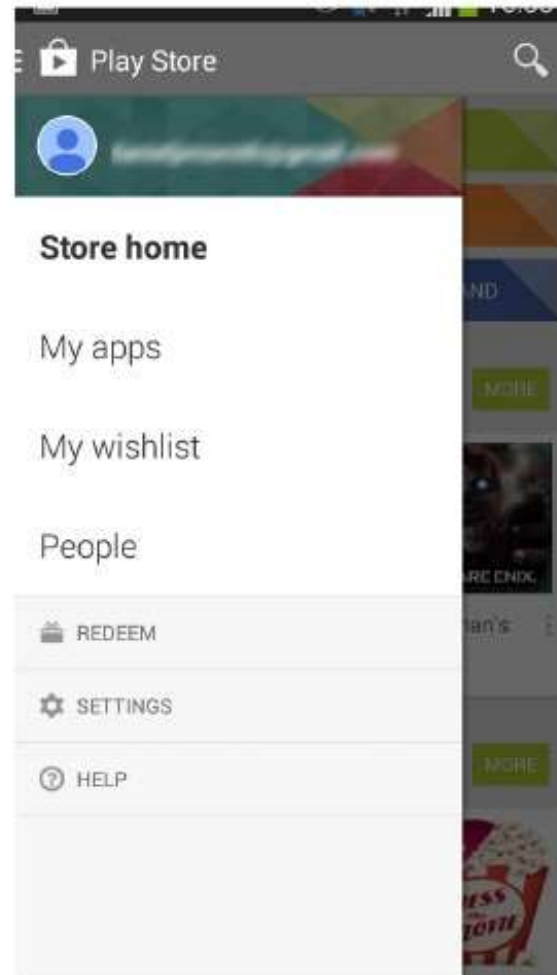


Android

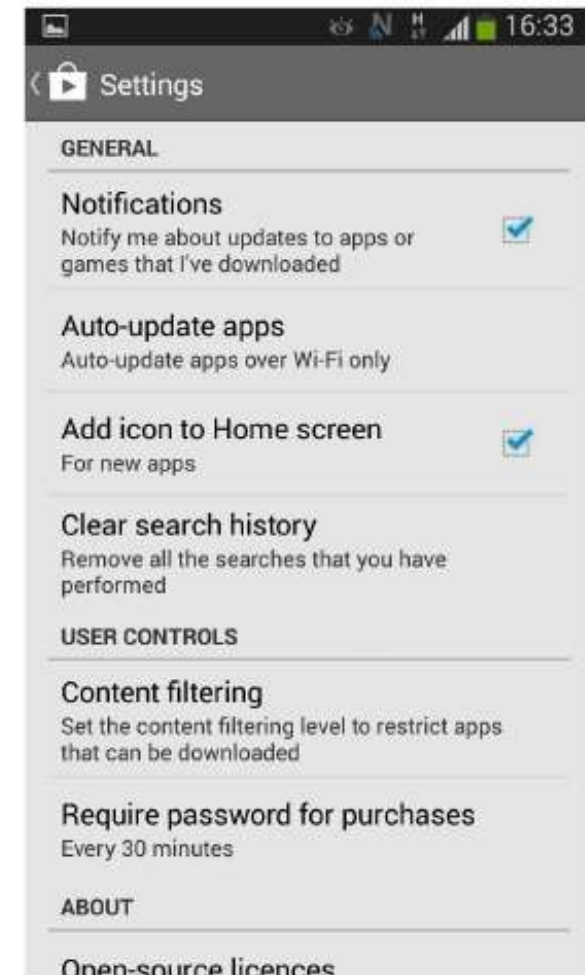
The settings in Google Play allow you to require a password for every purchase made in the Google Play store.



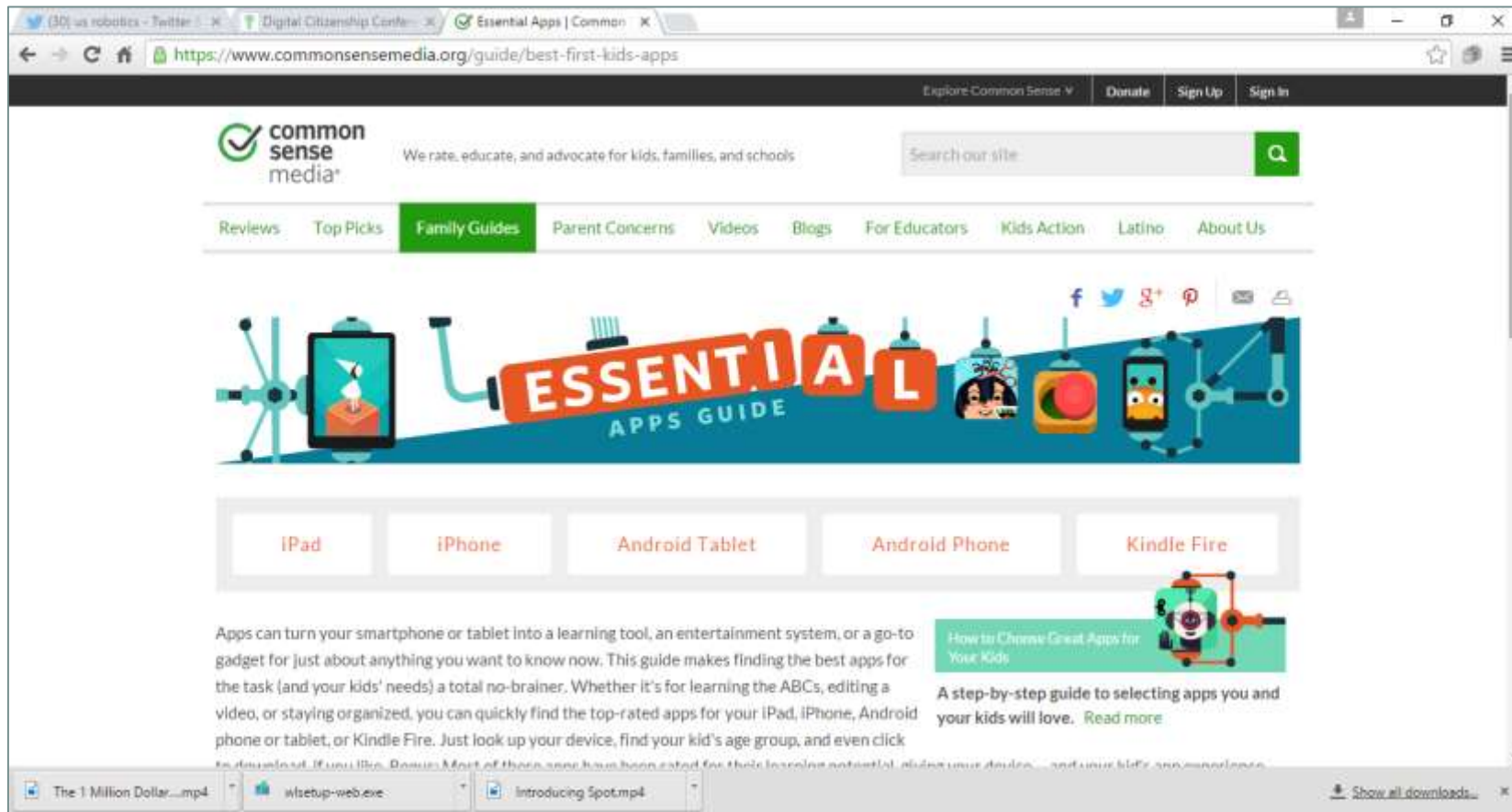
1. Go into the Google Play Store. Tap on the menu icon. Here it is located on the top left of the home page



2. Tap on Settings



3. Tap Require Password for purchases and then tap For all purchases through Google Play on this device.



NSPCC Netaware – Reviews of apps and games

<http://www.net-aware.org.uk/networks/?order=-popularity>

In association with





← Back to NSPCC site

O₂ 😊 NSPCC NetAware)))

Type and select network: >

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



Search for a site, game or app to find out more

>

Explore other networks

[All networks A-Z](#) [Most popular](#)



Where Families Make Sense of Video Games

Search

[STORIES](#) [CAREERS](#) [ADVICE](#) [RESEARCH](#) [ABOUT US](#) [ASK A QUESTION](#)

Jo Whiley introduces AskAboutGames.com gaming advice for parents



All About: Safe and Sensible



Join Our Family Gaming



Enjoy Games Safely With



ALL THEIR FAVOURITE SHOWS,
IN ONE PLACE.
WITH NO ADS. EVER.



Old Macdonald
had a farm





BULLYING

is the
REPETITIVE,
INTENTIONAL
hurting

of one
PERSON
OR GROUP



by



another
PERSON
OR GROUP

where
the relationship
involves



an
IMBALANCE
of
POWER



bullying can be
PHYSICAL



VERBAL or

PSYCHOLOGICAL



It's important that schools have a shared definition of bullying

PRACTICAL STEPS

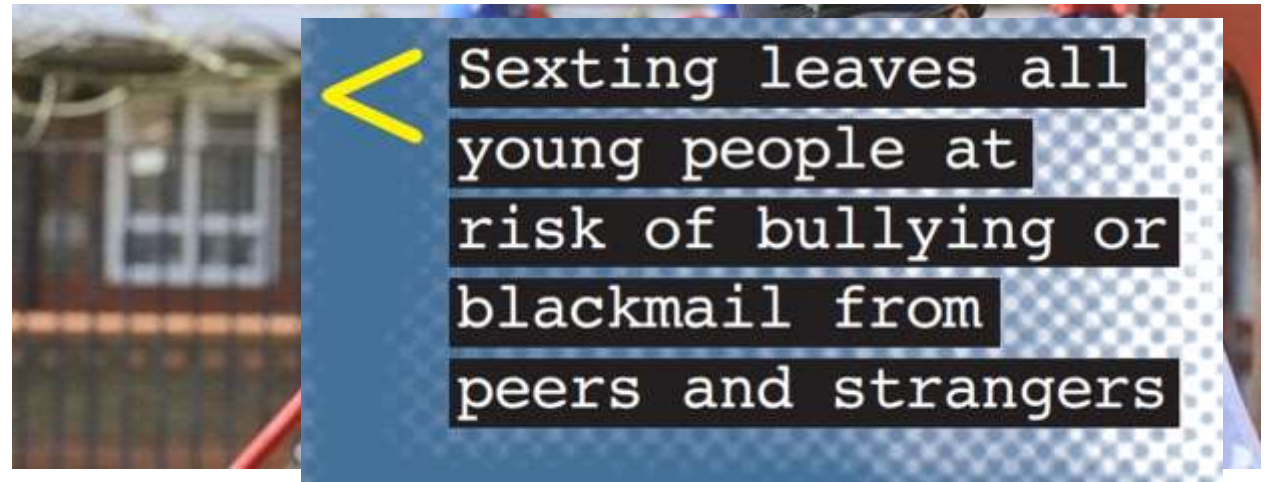
- ❖ Find out what exactly has been happening.
- ❖ Keep a record of all incidents and when they occurred.
- ❖ Take screenshots of any messages before deleting them.
- ❖ Block and report anyone who's been bullying your child online
- ❖ Change any passwords that might have been compromised by online bullying and check privacy settings.
- ❖ **Don't** confiscate your child's device or stop them spending time online.
- ❖ Make a plan for where your child can go to escape bullying at school.
- ❖ Make sure your child's school is aware – even if it's been happening outside school.



SEXTING

"The report of crime has been filed with the three children involved named and given an outcome of not in the public interest to prosecute." BBC 2015

A boy who sent a naked photograph of himself to a girl at school has had the crime of making and distributing indecent images recorded against him by police



National Police Chief Council's lead on children and young people, said if a school chose to take an incident to the police, then officers must record the crime.



REPORTING UNWANTED CONTENT



Criminal images can be reported to the Internet Watch Foundation www.iwf.org.uk Reporting to the IWF is confidential and can be done anonymously. The IWF deals with:

- child sexual abuse images hosted anywhere in the world
- criminally obscene adult content hosted in the UK
- non-photographic child sexual abuse images or videos hosted in the UK i.e. computer-generated or cartoon imagery

You can also report to content providers and ask them to remove hateful or overly sexualised content. Be prepared to quote back terms and conditions to get content removed



The Information Commissioner's website offers advice and support around privacy and data protection www.ico.org.uk

Also - Use flagging and reporting tools on websites

REPORTING UNWANTED CONTENT



If your child has been **inappropriately contacted by an adult** online – e.g. sexual chat, being asked to do something that makes them feel uncomfortable or wanting to meet offline – you should report it to CEOP www.ceop.police.uk/safety-centre

Child Exploitation & Online Protection Centre



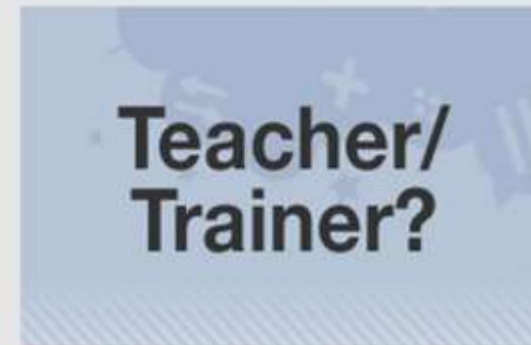
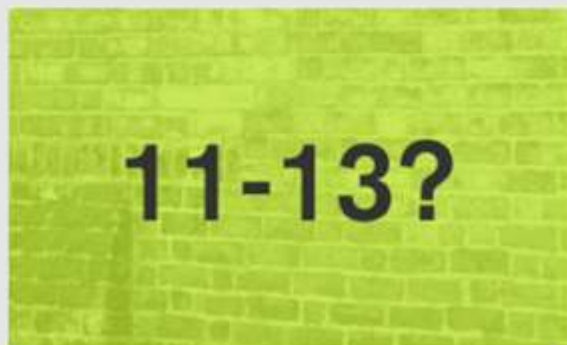
Parent Port brings together all of the media regulators and allows you to make complaints about online content www.parentport.org.uk/



Welcome to CEOP's Thinkuknow

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 or at home. 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 [NCA's CEOP Command](#). We hope you like it!

Are you...



SHARE THE

REN



Resources for 3-11s



Resources for 11-19s

KidSMART
a Childnet website

Visit Childnet's main website
www.childnet.com
for the latest resources and news

Childnet International

kidSMART | I work with kids | **I have kids** | Contact

Adventures of Smartie | Resources | Fun activities | Skills School | Know IT All | Internet devices | Parental controls | SMART Crew

I have kids

SIGN UP for our e-bulletin here

Read "The Adventures of Smartie the Penguin"

Download Childnet resources

Fun activities to try at home

Skills School

A parents' guide to Internet devices

Know IT All for Parents

Parental Controls

The Adventures of Kara, Winston and the SMART Crew (8-11)

the SMART Crew - films

Parental controls

Innocent searches online can lead to not so innocent results. But parental controls can help keep your child safe.



O₂ 😊 NSPCC

Let's keep kids safe online

PARENTAL CONTROLS - SHOULD YOU USE THEM?

Parental controls can be really useful, especially for parents of young or vulnerable children. They can help stop your kids seeing upsetting or inappropriate content before they're ready. But you may want to consider a few things before you set them up.

No tool is perfect

Under – and over – blocking

Long term wellbeing

Research out of the Oxford Internet Institute suggests that controlling your children's internet use too much could actually make them more vulnerable in the long term. Children who are very restricted when they go online tend to be less confident and able to deal with risk.

Make best use of tools to minimise the content your children are able to see, but do so in the certain knowledge that you cannot protect them from all the content that's online.

FILTERS AT HOME

Andrew K. Przybylski, Victoria Nash. **Internet Filtering Technology and Aversive Online Experiences in Adolescents.** *The Journal of Pediatrics*, 2017; DOI: [10.1016/j.jpeds.2017.01.002](https://doi.org/10.1016/j.jpeds.2017.01.002)

Oxford Internet Institute

WHAT DID THEY FIND?

Children are seeing images on smartphone apps, which means the use of filters inside the home may be out of date.

Filters are good at simple tasks like screening out swearing.

However a filter cannot know if a young person has known someone before it lets them start a chat on WhatsApp, or check what they're sharing.

Filters may also 'over-block' searches for information about issues that are important for teenagers, such as alcohol, drugs and sexual relationships.



PARENTAL CONTROLS

NSPCC

How to set up parental controls on...

Mobiles and tablets



Home broadband



Games consoles



Film, music and TV



Search engines



WiFi and being away from home



Apps and privacy



Helping parents keep their

Set up your
devices safely

SEE CHECKLIST >

Pre-school (0-5)

Resources for parents

Young Children (6-10)

Resources for parents

Pre-teens (11-13)

Resources for parents

Teens (14+)

Resources for parents

E-safety leaflets &
resources

Parents' guide to tech

Gadgets

Gaming consoles

Mobile phones

Tablets & Laptops

Televisions

Set up your child's devices
safely

Parents' guide to apps

Meeting new people &
chatting

Social networking

Entertainment & decoys

Child-friendly apps

Social networking

Online gaming

Social networking in
gaming

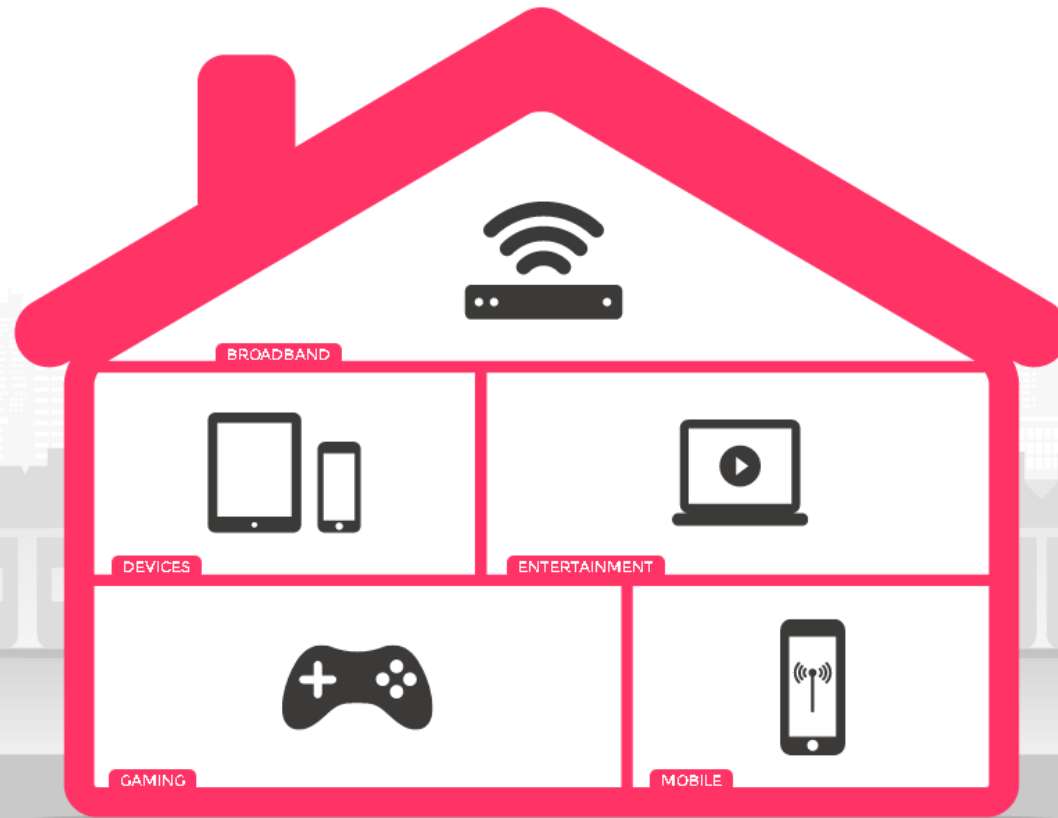
Downloading & viruses

Internet safety glossary

Texting dictionary



Protect your kids by activating
simple parental controls around your home



GET PROTECTED NOW >

PARENTAL CONTROLS — ALL DEVICES HAVE THEM

Here you'll find the relevant links to the parental controls instructions for the major devices.

Parental controls setup guides for the major tablets and smartphones:



Apple iPhone

Apple iPad

Android Mobile

Android Tablet

Parental controls setup guides for the major gaming consoles:



Xbox One

Xbox 360

PS3

PS4

Wii

Parental controls setup links for the main laptop and tablet operating systems:



Windows 7

Windows 8

Mavericks

Yosemite



<http://www.internetmatters.org/controls/devices-computers/>

PARENTAL CONTROLS OFFERED BY YOUR HOME INTERNET PROVIDER



We know that children, particularly younger children, can be bothered by things they see online, and filters can be a helpful tool in reducing the chances of coming across something upsetting.

Remember that filtering is only part of the solution

The 4 big internet providers in the UK – BT, Sky, TalkTalk and Virgin Media - provide their customers with free parental controls which can be activated at any time.

They have come together to produce helpful video guides to help you to download and set-up the controls offered by your provider.

<http://www.saferinternet.org.uk/advice-and-resources/parents-and-carers/parental-controls>

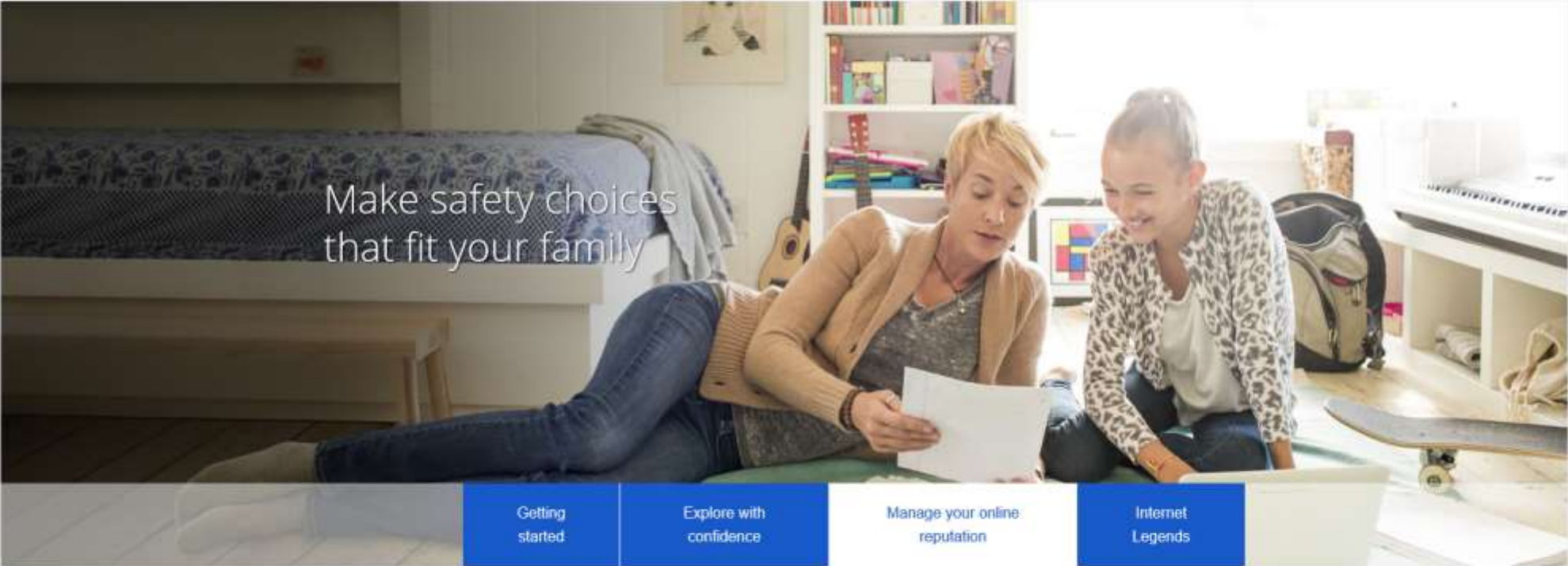


Manage your online reputation - For families - Safety Centre - Google - Microsoft Internet Explorer provided by Merton Domain

https://www.google.co.uk/safetycenter/families/manage/

Google Safety Centre

Home · For everyone · **For families** · Safety tools · Partners · Resources



Make safety choices that fit your family

Getting started · Explore with confidence · Manage your online reputation · Internet Legends

TOPICS

- Introduction
- Keep personal information on a need-to-know basis
- Make smart connections
- Be an upstander, not a bystander

Connect responsibly

From our ongoing conversations with parents, we know that staying on top of your teens' online activity is a big concern. Teaching your teen the basics of responsible digital citizenship will help them make good choices when you're not around. They should know how to respond to social media posts, texts, and other online messages.

SAFETY TOOLS

Discover Google safety tools designed to help your family monitor their online reputation.

Manage YouTube

<https://www.google.co.uk/safetycenter/families/manage/>

DIGITAL STRATEGY 01/03/2017



Government launches major new drive on internet safety. **27/02/2017**

- UK to be safest place in the world for young people to go online
- Parents now more concerned about their children sexting than drinking or smoking

Ministers have begun work on a new Internet Safety Strategy aimed at making Britain the safest country in the world for children and young people to be online.

The focus will be on preventing children and young people from harm online and making the internet a safer place.

HAVE A CONVERSATION

Talk about the good stuff, not just the bad.

Not sure where to begin? These conversation starter suggestions can help.

1. Ask your children to tell you about the sites they like to visit and what they enjoy doing online.
2. Ask them about how they stay safe online. What tips do they have for you, and where did they learn them? What is OK and not OK to share?
3. Ask them if they know where to go for help, where to find the safety advice, privacy settings and how to report or block on the services they use.
4. Encourage them to help someone! Perhaps they can show you how to do something better online or they might have a friend who would benefit from their help and support.
5. Think about how you each use the internet. What more could you do to use the internet together? Are there activities that you could enjoy as a family?

ATTACKS AND BOMBINGS

Hearing about attacks or bombings like the ones in London and Manchester, can make you anxious or scared. You might feel unsafe and if there are a lot of things in the news about the attacks, it can feel like the threat is massive. But it's important to remember that in reality, terrorist attacks are very rare.

Keeping you safe - what's happening?

- The police have made sure there are more officers in towns and public places like train stations.
- Airports have strict security checks and more security staff.
- Local communities are trying to teach people about world issues and safety.
- Public spaces like concerts, football matches and events have strict security.
- The government and police have specially trained workers who are always finding new ways to protect the UK.



Getting through a tough time

If you're struggling with something that's happened, we've got some advice to help

WHAT WE DO KNOW...

1. Building a child's digital resilience will keep them safer than blocking or filtering
2. Don't limit the talk you have with your child to 'the online safety conversation'
3. Balance taking an interest in your child's online activities with giving them the space to be independent
4. Don't be afraid to set boundaries
5. Concentrate on how children use digital media rather than for how long

TOP TIPS FOR SUCCESSFUL ONLINE PARENTING

"Good parenting is the single best way to keep your children safer online."

"Resilient children are more likely to set their own limits and safeguards. To do things like block users that are troubling them, or leave services that have content that upsets them."

WHERE CAN I GET HELP?

❖ <http://www.internetmatters.org/>

❖ <http://www.saferinternet.org.uk/advice-and-resources/young-people/3-11s>

❖ <http://vodafonedigitalparenting.co.uk/>

❖ <http://www.childnet.com/resources/kia/>

❖ <https://www.thinkuknow.co.uk/parents/> CEOP (Child Exploitation and Online Protection Centre)



DIGITAL PARENTING MAGAZINE

<http://www.vodafone.com/content/digital-parenting/learning-and-fun/digital-parenting-magazine.html#>

Please note, it is a very large file so make take some time to open.



SIX APPS YOU SHOULD KNOW ABOUT



SNAPCHAT



The photo messaging app allows users to take and share photos and videos, adding text and silly graphics to people listed in their smartphone's contact list who also have the app.

When Snapchat launched, its success came from the ethereal nature of the 'Snaps' – they lasted only a few seconds before disappearing and couldn't be saved by the person receiving them. This meant children could have fun, pulling silly faces and not worrying that the image would be around forever.

As Snapchat has evolved, this has changed. The person posting can now choose how long the images are available by creating Stories, which are available for up to 24 hours. Images can also be screen shot outside the app and shared by the person receiving them.

Snapchat is unmoderated and therefore, you cannot filter the posts your child receives or Stories they view, which means they can be exposed to adult content.

INSTAGRAM



Instagram allows its users to share images and videos with each other. It has recently introduced live streaming.

Users can comment on posts, which can lead to both positive and negative judgements.

Posts can be seen by anyone as default, but you can change your child's privacy settings so that only people they know can see them. However, their bio, profile and profile image will remain public.

Instagram has been accused of contributing to the rise in body image issues among young people. Celebrities post images that have been heavily edited, professionally styled and often retouched, giving an idea of beauty that is both unreal and unattainable for most people, while young people themselves can obsess over taking the perfect selfie.

MUSICAL.LY



Musical.ly lets you make and share music videos and its popularity has surged among children and young people, spawning its own young stars, rather in the manner of how YouTube launched the likes of Zoella and Alfie Deyes.

Users pick a song from within the app and dance or sing along, enhancing their videos with editing effects. They can then share their video or keep it private.

Because Musical.ly is an unmoderated live streaming app, parents should be aware that users can be viewed and contacted by others, including people they don't know. There have been reports of requests for images of a sexual nature from strangers commenting on children's videos.

Users can report abuse by tapping on the three dots icon (...) within the app and following the instructions. To block, go to the user's profile, click the three dots icon in the upper right hand corner of the screen.

YOUTUBE



Children and young people love YouTube. Some just like watching the clips – anything from Taylor Swift performances to cute cat videos to YouTubers like football gaming star KSI – while others make their own and post them for others to watch and comment on.

YouTube has simple parental controls to restrict access to adult content, strict community rules about posts and an easy process to report illegal, harmful or upsetting content. But there is still a chance your child will come across content you wouldn't want them to, including religious and extremist propaganda. That's why it's important to encourage them to think critically about anything they see on the platform. The content may not be true or have come from a verifiable source.

To post, you need to be 13 years old and open an account but you can watch content at any age. For children under 13, there is an app, YouTube Kids, with content specially curated for that age group.

SKYPE



Live streaming services like Skype allow users to broadcast in real time with no moderation.

Lots of families happily use Skype – it's a really useful app that can help people stay in touch with friends and relatives who live a long way away, or when parents are separated.

They can be used by people to communicate with children privately, which can be particularly worrying if your child uses them to talk to strangers online.

One of the problems for parents is that your child might not think their online friend is a stranger at all, so could be persuaded to do things they wouldn't normally, such as sharing sexual images, or become interested in extremist political or religious views.

Skype doesn't offer a facility to record conversations, but people could record them with a separate device or programme, and then share images without your child knowing.

Warn them of the dangers of using live streaming sites, and advise them that, if they do, they shouldn't give away anything that will identify their full name, where they live, like to hang out, or go to school when using these sites to talk to people they do not know in real life.

As with all sites and apps they use, teach them how to block and report, and make sure they have a trusted adult to confide in should something go wrong.

WHATSAPP



Another app parents are increasingly aware of because they use it themselves, WhatsApp allows groups of users to have a running conversation. It's good fun and can save a lot of time when organising activities – or even what the family is having for tea.

Children and young people use it to share images, organise homework and generally chat with their friends and they can communicate with anyone in their contacts list who has the app. It's aimed at 13+ (the age you could sign up came down from 16 after it was bought by Facebook, bringing it in line with its parent company's terms and conditions.)

There have been reports of bullying and inappropriate contact from adults on the app. It's unmoderated so young users will need to know how to block upsetting or illegal contact and report users within the app themselves.

99

1. Problems
2. Being Flaky
3. Almost 100% Certain
4. Parent Stopped watching

99 means parent watching and can also be written as CD9 (Code 9).

Two nines written as 99 means that they have stopped watching and have left the room.

Other ways of writing that parents are watching include @@@, PAW (Parents are watching), PAL (Parents are listening), PIR (parent in room), PWOS (parents watching over shoulder).

| 182

1. Hit the bullseye with two darts remaining
2. Don't blink, I'll be right back
3. I'm thinking of...
4. I hate you.

1 = I, 8 = hate 2 = you.

| KMS

1. Kiss me slowly
2. Kilometres
3. Keep my Secret
4. Kill my self

KMS is used to mean kill myself although usually not a literal threat to commit suicide but more as an exaggerated form of annoyance, e.g.: “My mum won’t let me go to the party this weekend... KMS”

MIA

1. Mum is About
2. Message if alone
3. My Internet Age
4. Bulimia

Worryingly, Mia is a nickname used to discuss the eating-disorder Bulimia in online chat-rooms and forums. Ana is also mentioned when referring to Anorexia, another type of emotional disorder characterised by an obsessive desire to lose weight by refusing to eat. Often, the terms “Goddess Mia” and “Goddess Ana” are dropped in online conversations where tips on losing weight are discussed predominantly by young female teens.



1. I've just seen something x- rated
2. She didn't even see me
3. I can't see your point of view
4. I'm so tired I'm cross eyed

This emoji is often used in online chats when something NSFL (not suitable for life) has been posted or discussed.

@derekcrabtree1



Should you be afraid? – No
Should you get tooled up - Yes

