







Helping to keep your children safe online



## "Helping to make the internet a great and safe place for children"

Promoting the positive



Responding to the negative

Adults often have anxieties about new media...



Everything that's already in the world when you're born is just normal;

## Different world?





"Anything that gets invented after you're thirty is against the natural order of things and the beginning of the end of civilisation as we know it ...until it's been around for about ten years when it gradually turns out to be alright really."

**Douglas Adams** 

Why is internet safety important?



Why is the internet so great?



What are the risks?



What about mobiles?



Know IT All - what can parents do?



# Why is internet safety important?

### **Statistics**

- The amount of time 8-11s and 12-15s spend online has more than doubled since 2005... The amount of time 8-11s and 12-15s spend online has more than doubled, from 4.4 hours a week in 2005 to 11.1 hours
- However, there has been a decrease since 2014 in the number who trust their child to use the internet safely Since 2014, parents of 3-4s (44% vs. 56%), and 5-15s (78% vs. 83%) whose child goes online are less likely to say they trust their child to use the internet safely.
- Parents are more likely in 2015 than in 2005 to believe that their child can get round parental controls In 2005 very few (5%) parents who were using blocking controls or software said their child knew how to get around those controls. In 2015 29% of parents of 8-15s said they thought their child would be able to unset, bypass or over-ride home network-level filters, and 21% thought this about parental control software.

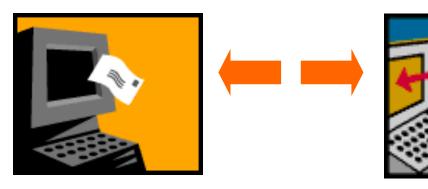
## Different usage

#### **PARENTS**

Mostly email & web for research

#### YOUNG PEOPLE

Interactive chat, IM, Music, Games, Blog



## Know IT All

28% of parents who use the internet describe themselves as beginners compared with only 7% of children

## Changing environment

WEB v 1.0

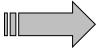
WEB v 2.0

**Downloading** 



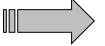
+ Uploading

**Consuming** 



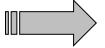
+ Creating

Corporate



+ Personal

Separate media



+ Converged media

**Static** 



+ Truly interactive



#### IN SCHOOL

Supervised, filtered & monitored

## Supervision



#### **OUT OF SCHOOL**

Often no supervision, filtering or monitoring



## Know IT All

- >30% of students report having received no lessons at all on using the internet.
- >79% of young people use the internet privately without their parent's supervision

## Knowledge vs. Wisdom

#### **KNOWLEDGE**

Many children pick up technology quicker!



#### **WISDOM**

Understanding how to behave in a virtual world

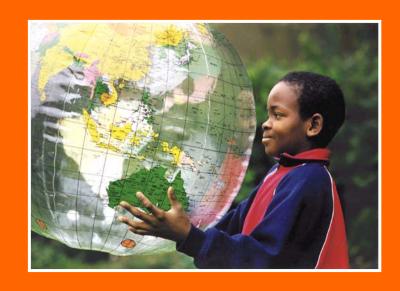


## Know IT All

69% of young people say they mind their parents restricting or monitoring their internet usage!



Why is the internet so great?



## **Discover**



- Search engines
- Homework
- Projects
- Personal interest
- Amazing facts

The biggest library in the world

## Connect



- Email/chat
- VolP Skype
- Instant Messenger
- Multi-user games
- Social networks

Brings people together

## Create



- Blogs (web log)
- Vlogs (video log)
- Web sites
- Text & pictures
- Music/photo/video

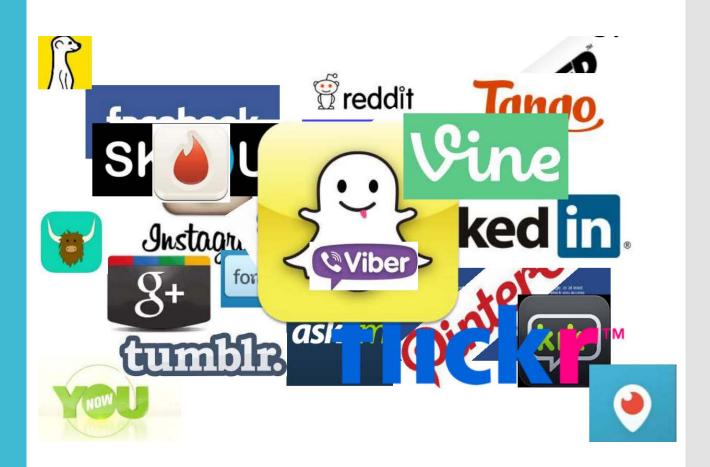
Anyone can become a publisher

# ROCKIDS

Connect: Instant Messenger (IM)

- •This app is meant for kids below the age of 13 and to be used under parental supervision
- •A parent creates the kid's account and gets to choose the kid's username
- Parents can set 'Curfew Time' during which the live chat will not work

Connect: Social networking sites

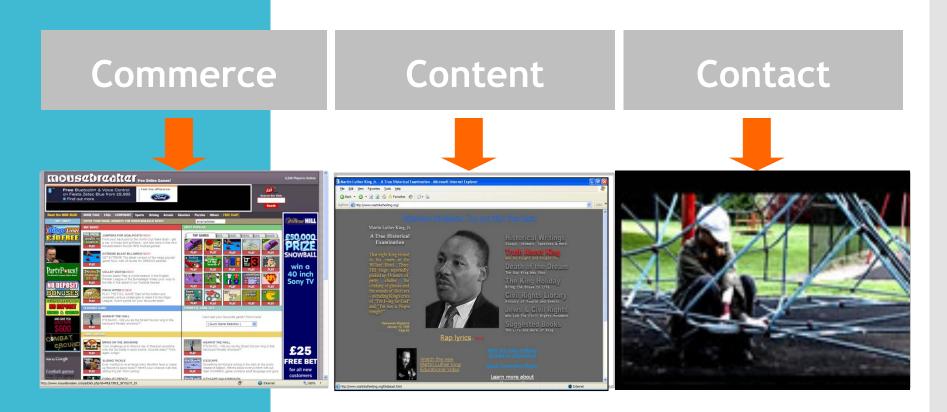




## What are the risks?



### Potential risks



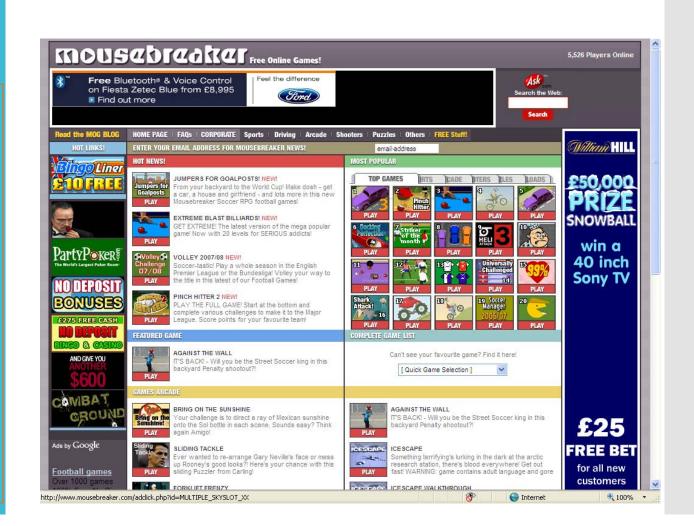
73% of online adverts are not clearly labelled making it difficult for children and adults to recognise them

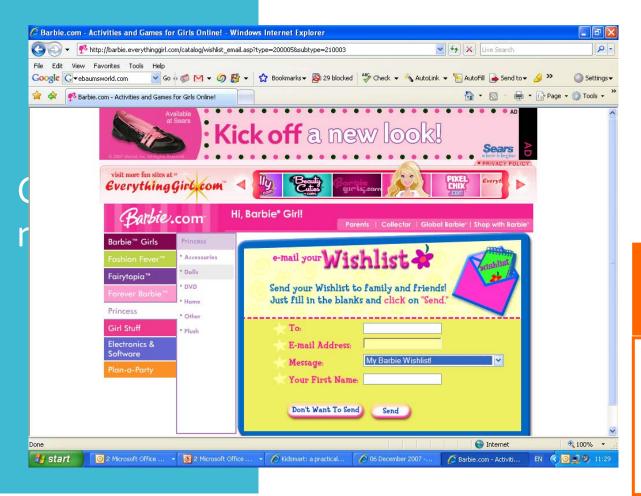
57% of 9-19 yr olds have come into contact with online pornography accidentally.

- 4 in 10 pupils aged 9-19 trust most of the information on the internet. 1/3 of young people have received unwanted sexual or nasty comments online. Only 7% of parents think their child has received such comments.

## Commercial risks

- Blur between content & advertising
- Subtle requests for marketing information-"Tell a friend"
- Invasive programmes adware/popups





## Know IT All

20% of children claim they mustn't fill in online forms, compared with 57% of parents who do not allow it.

## Content viewed

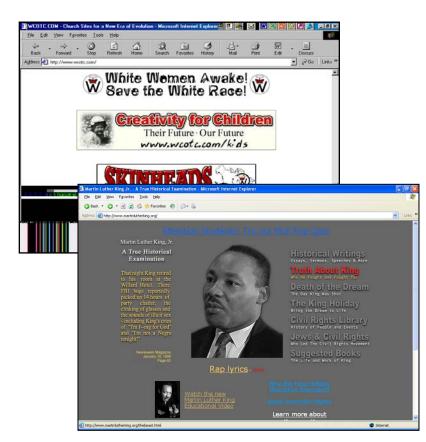
- ⊗ Inaccurate content
- Extreme material
- Pornography
- **⊗** Fake News



## Know IT All

4 in 10 pupils aged 9-19 trust most of the information on the internet

57% of 9-19 yr olds have come into contact with online pornography.
Only 16% of parents think that their child has seen pornography on the internet.





## Contact risks

- ⊗ Social networking sites
- Instant messaging (eg Whatsapp, Snapchat, messenger)
- ⊗ P2P (filesharing)
- Multi-user online games
- Chat rooms

## Know IT All

49% of kids say that they have given out personal information 5% of parents think their child has given out such information

NOW

Connect: Social networking sites







Talk to strangers!

## Live.ly music.ly

Live.ly, the live-streaming video app, is relatively new. It was released in May and racked up more than 2 million downloads in a month. As we've all seen, there's a soaring popularity for live-streaming social media with Twitter's Periscope and Facebook Live. While musical.ly focuses on music, live.ly gives musers free reign on what they want to share with fans and allows musers to communicate with fans in real time. Musers can pick from a variety of categories, including makeup, life, sing, dance, etc., to tag in their live videos.

#### So are these apps safe?

Probably. You'll want to make sure your child disables location services for the app in his or her phone settings. Then in the app, you'll want to turn on three tabs in the app settings:

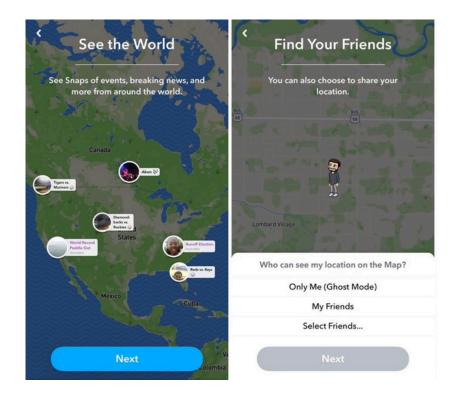
- 1. Only friends can direct.ly me
- 2. Hide location info
- 3. Private account

For live.ly, stress the importance of being smart while using the app. Live streaming is exactly what it sounds like; your kid will be live on the Internet, without the ability to edit the video before others see it. Location of the live-stream is also crucial as it can give away information about where your kid lives and spends time.

Musical.ly is obviously a music-based app, but not all the songs are kid friendly. There are dozens of song categories to pick from and what seems like millions of songs, so your kid probably isn't going to be singing Disney songs.



## Snapchat





office@bredhurst.kent.sch.uk : www.bredhurstcep.co.uk



Gilling Kent ME7 3

Tel: 018

26th January 2018

myone aware of this app? ROBLOX.

#### Dear Parents

The teachers spoke to the children yesterday regarding this app. Most of the children had either played it or were aware of it.

#### PLEASE SEE MESSAGE BELOW FROM KENT POLICE.

Warning: We are putting out this post following our visit to a school yesterday. As most people know we are concerned about the popular app ROBLOX which is by far the most popular game played by children from 5 to 10 years of age.

We were talking to a very large group of year 1 students and we were shocked when over half of them said they were playing ROBLOX. When we spoke to Year 2 at least 70 percent of them were playing the game.

Most of these children then disclosed that they had online friends in ROBLOX that their parents didn't know about. It got worse when many of the children stated they had received many in game messages from 'strangers' and that they hadn't told their parents. All of the children then stated that they had seen 'naked' characters walking around the game and that the characters were doing very adult things. The inappropriate content has been disclosed to us thousands of times by young children but we were previously unaware that the children were being sent numerous messages. When talking to Year 3 students they suggested that a lot of the messages are inappropriate. In all cases the children aren't telling their parents.

Most of the young children we spoke to yesterday appear to have been talking to strangers in the game by using a headset to speak. The headset is usually just a normal set of ear pods that you would get bundled with an Apple device as opposed to a specific gaming accessory.

We would advise every parent to check their child's ROBLOX account and look to see if they have friends that they do not know. Many of the children we spoke to yesterday said their accounts were "maxed out" meaning they have 200 online friends.

We would also ask parents to check the child's in game message inbox to check if they have been secriving inappropriate messages.

PLEASE CAN EVERYONE SHARE THIS POST SO THAT PARENTS KNOW TO CHECK THEIR CHILDS ACCOUNT

Best Wishes

#### Dear Parents and Carers

It has come to our attention that many of the children are playing on-line games with each other. This means they can communicate and share the experience, which is an excellent way to communicate and encourages sharing, cooperation and collaboration. However, it comes with many risks that young gamers may not have considered. We have reason to believe that some of our pupils are sharing significant information that may have a financial impact and could risk parental on-line security.

#### Risks of Game-Sharing on Xbox/Play Station

Game sharing is a way to take advantage of the Dual License that comes with each purchase of a Digital Game - it can be played on more than one machine. The sharing happens when two people online share games for free.

To game share, players have to share account usernames, passwords and verification codes. Sharing personal details is highly inappropriate, breaks many terms of use (as outlined in Service Agreements) and can result in players having their account frozen by their provider or even stolen from them by strangers.

More importantly, many young gamers play on parental accounts. These accounts will probably have been set up by parents using their own passwords and user details. Children may be sharing passwords used on various family member on-line accounts and can allow children to share accounts. This can evolve into sharing purchase passwords and even access into bank accounts, especially if you use the same password for a number of different applications, including PayPal, Apps, Spotify etc etc.

Finally, once these personal details are shared on-line, there is no limit to who they can be shared with next. Once it has left your device - you have no control.

We will be talking to the children in KS2 about their on-line activity, but obviously parents will need to closely monitor what is happening in the home to ensure you are not compromising your own on-line or financial security.

## Blue Whale Game?



## Nelson Primary School Inspiring Ambition, Achieving Success

Head Teacher: Mrs F. Cullen Deputy Head Teacher: Ms J. Cull School Business Manager: Mrs S. Silk Napier Road, East Ham, London, E6 2SE Telephone: 020 8472 0642 Fax: 020 7345 1816

E-mail: info@nelson.newham.sch.uk Website: www.nelson.newham.sch.uk fax@nelson.newham.sch.uk

Dear Parents / Carers,

#### Blue Whale Game

I would like to warn you about a very dangerous game that a lot of the children are talking about. You can access this game from social media sites like Instagram, Facebook Snapchat etc.

In the game the people who run it are called "Masters." The masters send tests or challenges through to the person playing the game and take place over 50 days. They start quite small such as wake up at 4.20 or watch a horror film. The challenges get worse and worse until they are asked to carve the shape of a blue whale into their own skin. To win the game the player is asked to commit suicide; if the choose not to do that the player is told that the masters will kill their family

Please keep an eye on your child and talk to them about the dangers of games like this one. I would also like to point out that no child in primary school should have a social media account such as Instagram or facebook. The lower limit for these sites is 13 years old.

Yours faithfully,

Hara C Carlo

Fiona Cullen Head Teacher Apps – where?



Apps lock & Gallery hider

Calculator%.

**Audio Manager** 

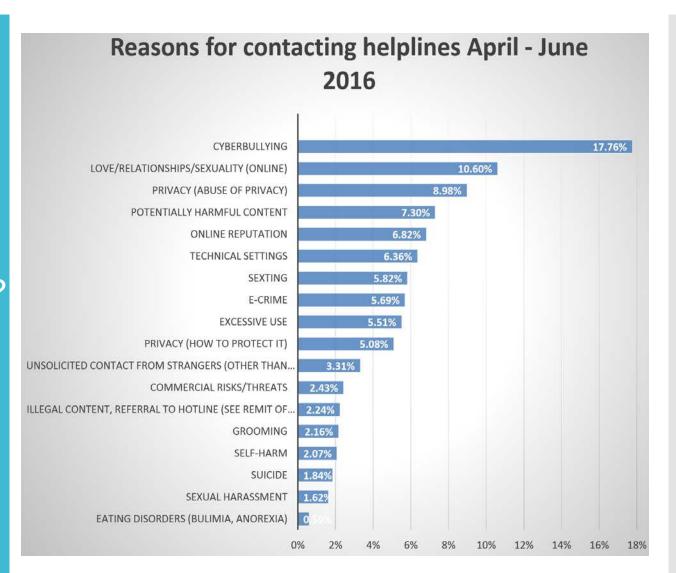


# 3

Over to you...

What do YOU think is the biggest risk to children online?

## Cyberbullying?



**Prejudice** 

Hacking

**Threats** 

**Manipulation** 

What is Cyberbullying?



**Exclusion** 

**Stalking** 

**Public postings** 

- Threats and intimidation
   Threats sent to people by mobile phone, email, or online.
- Harassment or stalking Repeated, prolonged, unwanted contact or monitoring of another person.
- Vilification / defamation / prejudice-based bullying
   These may be general insults or racist, homophobic or sexist bullying.
- Ostracising / peer rejection / exclusion
   Set up of a closed group refusing to acknowledge one user on purpose.
- Identity theft, unauthorised access and impersonation
   'Hacking' by finding out or guessing a username and password.
- Publicly posting, sending or forwarding information or images
   Disclosing information on a website.
- Manipulation
   May involve getting people to act or talk in a provocative way.



## Differences



- 24/7 contact
   No escape at home
- Impact
   Massive potential audience reached rapidly. Potentially stay online forever
- Perception of anonymity
   More likely to say things online
- Profile of target/bully Physical intimidation changed
- Some cases are unintentional Bystander effect
- Evidence Inherent reporting proof

## Advice for parents

- Be careful about denying access to the technology
- Understand the tools
- Discuss cyberbullying with your children
  - always respect others
  - treat your passwords with care
  - block/delete contacts & save conversations
  - don't reply/retaliate
  - save evidence
  - make sure you tell
- Report the cyberbullying
  - school
  - service provider
  - police



## What about mobiles?



## The pros and cons



Discover Connect Create

Commerce Content Contact



**Portable** 

Away from supervision

Always on and reachable

## Mobile phone advice

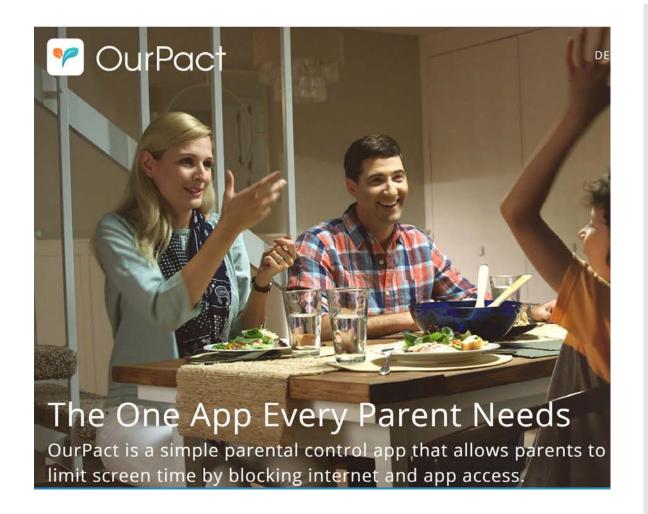
- Know how your child's phone works (e.g. Bluetooth, Internet access, WIFI code)
   Agree the type of content that you would be happy for them to download, knowingly receive or send on to others
- Save any abusive messages/inappropriate
- images for evidence purposes

  Decide together what are acceptable bills inc In-app purchases

You can control spending on in-app purchases by turning them off completely or by asking for a password to be entered every time. This will mean that your younger children won't be able to download apps without your permission.

- Some free apps make money in different ways, building up bills without you even realising it. PhonepayPlus has more information on in-app purchasing.
- Encourage balanced use switching off at mealtimes, bedtime.

Apps – who is in charge?



## Apps – who

is in charge?

SelfieCop reminds kids to STOP-&-THINK before taking or sharing photos or videos.



For example, the Parental Control SelfieCop teaches kids to use their phone's built-in camera safely.



**SelfieCop** reminds kids that any photos or videos they take may ultimately be seen by anyone.

**SelfieCop** also allows parents to monitor their child's images to help safeguard behaviour.

Download the SelfieCop apps for free at www.selfiecop.com

# Update yourself!

#### Parents warned to delete app ooVoo from their children's smartphones

15:09, 15 MAR 2016 UPDATED 15:57, 15 MAR 2016 BY EMMA GILL The warning comes from school bosses after pupils were sent explicit images on the

Children in North East Lincolnshire targeted by online sex pests using ooVoo



√ View all networks



#### ooVoo

Voice calls | Video chat | Messaging



#### Minimum age

What do you think is the right age for ooVoo? Share your thoughts~

ooVoo is a video chat app. It lets you make video calls, voice calls and send texts to friends and family. You can also start a group video chat with up to 12 people. The default privacy settings are set to 'public', so you can talk to people you don't know, but they can be changed so that you can just talk to your friends.

#### What do I need to know about ooVoo?

We've joined forces with O2 to find out what parents of 8-12 year olds think about ooVoo. We've also asked young people what they think. Here's what they said:

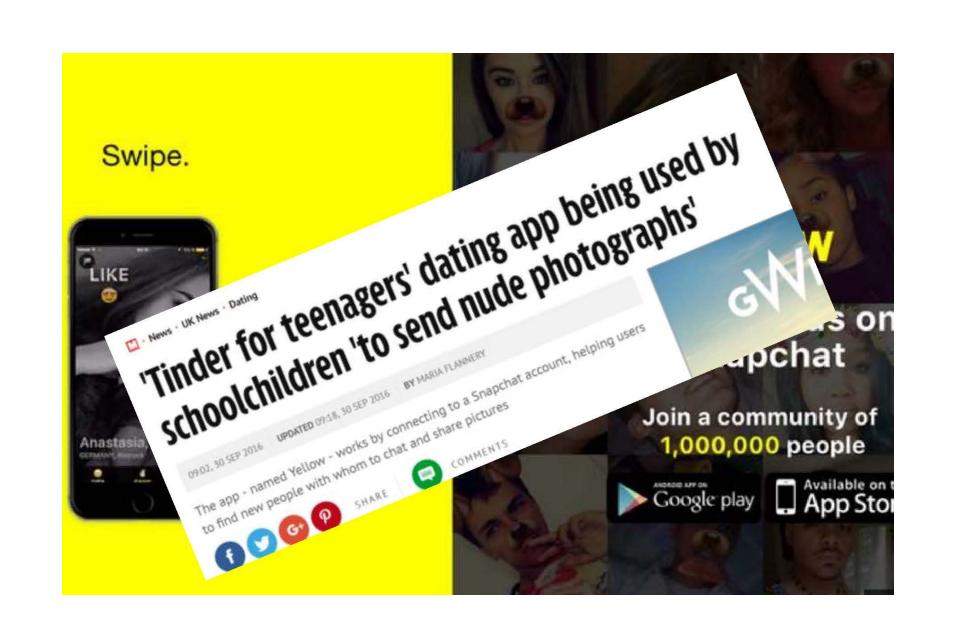
#### Children's views



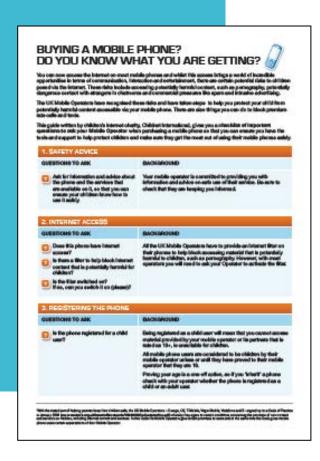
#### What do children and young people say to look out for:

23% of the children and young people we asked think ooVoo can be risky. The top 3 concerns were:

- · some of the features lag
- · talking to strangers
- · advertising.



# Checklist of questions for mobiles



## **Mobile Operators Code of Practice**

Services to protect children that operators are committed to including.

### Childnet's Checklist for parents

To help parents ensure that these protections are in place. Questions include: How can I turn Bluetooth off? Can I put a bar on premium numbers?



# What can parents do?



Reviews

Top Picks

Family Guides

Parent Concerns

Videos

Blogs

Education

Kids Action

Latino

Donate

#### Parenting, Media, and Everything In Between



O, (i) NSPCC Net Aware))

Type and select network

Q (e.g. Facebook)

Explore all networks

A-Z Most popul

## Got a question?

Whether you want to set up parental controls, adjust privacy settings or get advice on social networks, experts from the O2 & NSPCC are here to help.

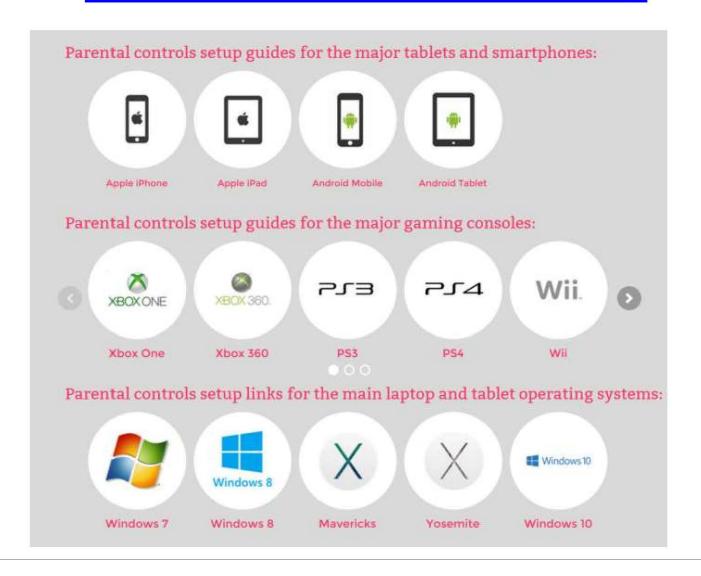
0808 8005002

## Your guide to the social networks your kids use

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



## www.internetmatters.org



## What you can do...

#### Commerce



- Install software to protect your computer's security
- © Be careful which sites the rest of the family visit
- © Use a family email address for shopping and online forms
- © Use the free technology: pop-up blockers & SPAM filters; and your good judgement: don't reply to SPAM!
- © Check sites for extra security (Green padlock)

# What you can do...

#### Content



- ©Talk to your children about what to do if they do come across something unpleasant and teach them to be critical. LITTLE & OFTEN!
- ©Use child-friendly search engines or set a search filter
- © Encourage them to use browser tools Bookmarks & History
- Install filtering but don't rely on it
- ©Find appropriate sites to visit and try not to overreact lots of inappropriate content viewed accidentally

#### Contact

# What you can do...



- © Get involved with your children online and encourage balanced use set time limits
- Make sure they know who to talk to if they feel uncomfortable
- ©Talk about the consequences of giving out personal info or making information public
- © Keep the usage in a family room
- Agree rules as a family meeting up



#### **SMART** rules



**SAFE** - Keep safe by being careful not to give out personal information - including full name and email address - to people who you don't trust online.



**MEETING** - Meeting up with someone you have only been in touch with online can be dangerous. Only do so with your parent's/carer's permission and even then only when they can be present.



**ACCEPTING** - Accepting e-mails, IM messages or opening files from people you don't know can be dangerous - they may contain viruses or nasty messages!



**RELIABLE** - Someone online may be lying about who they are, and information you find on the internet may not be true. Check information and advice on other websites, in books or ask someone who may know.



**TELL** - Tell your parent/carer or teacher if someone or something makes you feel uncomfortable or worried, or you or someone you know is being cyberbullied.

# Know where to report





If you click on the button you will be reporting a problem directly to someone at CEOP (the Child Exploitation and Online Protection Agency) You are then likely to be contacted by a social worker or a police officer, to talk through your report in more detail. They need to do this to make sure you are safe.



## Reporting

#### Reporting on social media

Find out more about how to report on the most popular social media apps in our safety tools guide.

Grooming or other illegal behaviour:

If you want to report someone who is behaving suspiciously online towards a child, you should in an emergency contact the emergency services by calling 999, or otherwise make a report to CEOP, the Child Exploitation Online Protection Centre, see www.ceop.gov.uk.

#### Criminal content online:

Child sexual abuse images: If you stumble across criminal content online, you should report this to the Internet Watch Foundation at www.iwf.org.uk/report. Criminal content in the UK includes child sexual abuse images, criminally obscene adult content as well as non-photographic child sexual abuse images.



Online terrorism: You can report terrorism related content to the police's Counter Terrorism Internet Referral Unit at www.gov.uk/report-terrorism.

Hate speech: Online content which incites hatred on the grounds of race, religion, disability, sexual orientation or gender should be reported to True Vision at www.reportit.org.uk.

#### Media content inappropriate for children:

If you want to make a complaint about an advert, television or radio programme, film, newspaper, magazine, video game or other type of content that you think is unsuitable for children to see or hear, you can report it through ParentPort at www.parentport.org.uk. Click on Make a Complaint and ParentPort will take you straight to the right place to complain to.



More resources...

www.childnet.com
www.kidsmart.org.uk
www.digizen.org
www.nspcc.co.uk











