

Online Safety

Social Media & the Dangers

Jonathan Taylor MSc

Internet Safety Consultant

www.besafe-online.co.uk

Keeping Up To Date with your childs
Online Behaviour
&
Keeping Your Child Safe on the Internet
'Risk – Danger – Harm'

Online Safety Options Open to 'Society'

• Parents / Carers

Educate Parents / Carers on the possibility of Risk-Danger-Harm through online interaction by Children, as a result of Inappropriate Contact-Content-Conduct.

ENCOURAGE - DIALOGUE & ONLINE PARTICIPATION

• Educators

Educate 'educators' on online trends of children , social media File sharing, gaming, etc that MAY result in Danger & Harm from sexual, physical, emotional, psychological or reputational exploitation

ENCOURAGE - DIALOGUE & 'BYOD' DAYS & UNSTANDING VULNERABILITY

• Industry/Organisations

Educate all on online trends that can assist in effective, policing, and understanding of the Risks & vulnerability that can escalate to Danger & subsequent Harm. Furthermore encouraging dialogue, blocking & filtering. & co-operation

ENCOURAGE - DIALOGUE & CO-OPERATION

• Children / Young Adults

All users should be educated about the difference between Risk-Danger-Harm & the possibility of Danger through 3 C's & possible subsequent exploitation

ENCOURAGE - EMPOWERMENT UNDERSTANDING DIALOGUE WITH PARENT/CARERS/TEACHERS

London E-Safety Survey

2013 (17,000 Children 9-17)

The main conclusions of the survey were:

The majority of children enjoy using the internet and have little concerns

A child's home is where they have most online access and face risks, and this will only increase with widening smartphone access

Online Bullying is their most significant worry when using the internet

Gender stereotypes are at their strongest online

Boys are as much at risk as Girls

Parents' awareness and knowledge of the internet is very important, as is teachers'

Schools should embed an e-safety programme throughout all year groups, and ensure children know how to report concerns

Schools should keep parents and carers advised on e-safety at home

Do not assume that risks increase with age.

What are the risks?

Sharing personal information

- i. Online profiles / Twitter / Facebook / Snapchat / Apps
- ii. Sharing too much information with friends and strangers. **(SYNC)**
- iii. Address, phone numbers, email addresses and locations **(GPS)**
- iv. Photos and status updates.
- v. Checking In – Like – Poke – Status – Location – Upload **(GPS)**

Online Social Media Behaviour –
Offline Awkwardness



Spectrum of Digital Knowledge / Usage / Understanding

←————→



Like many of you in this room, I'm a digital immigrant... My two young daughters, on the other hand, will be digital natives. They'll never know a world without ubiquitous broadband internet access... We may never become true digital natives, but we can and must begin to assimilate to their culture and way of thinking.
- Rupert Murdoch, April 2005

Digital Immigrant



Digital Native

Remember : Immigrants Always Learn from Natives

Social Media - Risk – Danger - Harm

Risk	Downloading and use of Apps or websites Windows – IOS - Android
Danger	Illegal or Inappropriate Online behaviour Content – Contact - Conduct
Harm	Emotional Sexual Physical Online Exploitation Online Reputation Damage Illegal Behaviour

If you can describe risk & explain risk you are in a better position to protect and control it'

Minimising Risk can Reduce the Escalation to Danger which in turn drastically Reduces possible Harm

Risks

can lead to

Dangers

can lead to

Harm

Harm = Exploitation

including:

- Physical Exploitation
- Sexual Exploitation
- Emotional Exploitation
- Reputation Damage
- Radicalisation / Extremism
- Bullying
- Identity theft / Illegal behaviour
- Exposure to inappropriate content
- Obsessive use of ICT
- Copyright infringements

Risks In Everything Online – However-
Only Dangerous as a Result of
Inappropriate Content / Contact / Conduct

I. Social Media / Access & Usage

II. Social Networking – Interaction Sites & Apps

III. Sexting / Sexcasting (Sexy Selfie)

IV. Cyberbullying / Trolling / Revenge

V. Online Reputation / Digital Tattoo

Must Understand Online Behaviour to Understand Risk & Prevent
Escalation

MUST DEFINE ACCURATELY TO EDUCATE EFFECTIVELY

Cat Fishing

What Worries you?

Spoofing

Over Use

Ratting

Addiction

IG Pics

Hacking

Theft

Vamping

Selfie

Newspaper headlines are a great Conversation starter with your child

3

What adults worry about

- Predation (Sexual Emotional Physical - Grooming)
- Viewing inappropriate content
- Posting/sending inappropriate content (Sexting / Sexy Selfies etc)
- Cyberbullying / Trolling & harassment
- Copyright Theft
- Online addiction
- Online Conduct contributing to destructive, illegal or inappropriate behaviour
- Online Reputation & Identity – Digital Tattoos

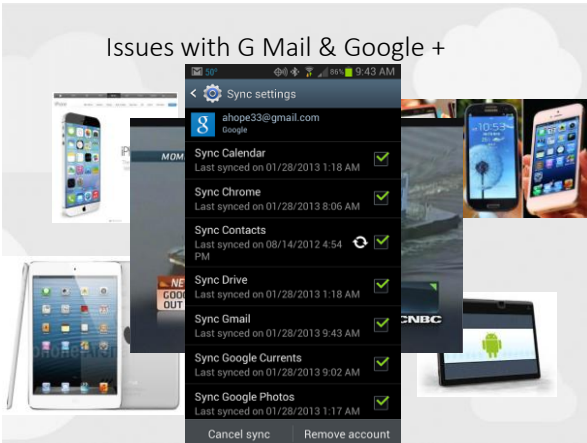
Logout
is the hardest
button to click.



Risks – Danger - Harm Operating Systems



Issues with G Mail & Google +



What do Apple, Facebook, and Google Know About You?

Facebook

FB allowed to share, sell, store info how it likes Name – Birthplace – City of Residence – Phone – Email – Current Employment – Relationship - Anniversary – Previous Relationships – Aliases- Screen names- Address Book – Family members – Religious Views + Much More (Like Button is Tracked) FB Apps know who you are talking with etc

Google

Google allowed to share, sell, store info how it likes Location On – Google Tracks History On – Google Tracks hourly- daily-monthly activity- top clicks / queries/sites Age, gender, predicts your interests. - Tracks devices you use & when last active – Tracks how many emails sent and how many contacts/ documents you have- Tracks all talk accounts

Apple

Apple allowed to share, sell, store info how it likes Name – Address – Email – Credit Card Details – Employment – Real time location – Habits – Use Cookies for Advertising – Tracks Safari pages – Siri – is recorded sent to Apple and transcribed to process request Contacts – Songs LOCATION LOCATION



What are children doing online?

Online Gaming

- i. Playing games against friends and strangers.
- ii. Chatting to friends and strangers using microphone headsets.
- iii. Exchanging contact details.
- iv. Playing games unsuitable for their age?
- v. Tiredness v Addiction



Grand Theft Auto – inappropriate
Contact Content & Contact
Visual & Audio



Webcam Abuse



Convincing young people into doing sexual things on webcam.

Exploitation from Deliberate Inappropriate Use

Exploitation from Unknown Webcam Access

Victims - can happen to boys and girls.

Remote Baby Monitor

Access & Recording- Viruses





Video Sharing Sites

Popular video-sharing sites/Apps:

- YouTube
- Vimeo
- Justin.tv
- Oovoo
- Vine
- Keek
- You Now
- Kik Video
- Periscope
- Chat Roulette / Omegle / Cam Frog etc

Users view and post videos (live or archived)

Post and read comments about the video content.





What are children doing online?

Music/Film Streaming and downloading

- Downloading music legally
- Downloading music illegally
- Uploading music
- Streaming music (Spotify)
- Downloading Films (File Sharing Systems)
- Streaming Films







Bullying + Technology = Cyberbullying

'The Way we Hurt Has Evolved'

2.31

Inappropriate Conduct?

Cyberbullying

- i. Bullying someone using **technology**.
- ii. It is a big problem having migrated from Messaging to Apps (DM's).
- iii. It can start off as a joke and spiral out of control.
- iv. Fraping always an issue
- v. It can be very **malicious**.
- vi. Adults and young people think that because its online it gives then **anonymity**.
- vii. It now almost always involves **'The Camera'**
- viii. Mostly through **Apps (YikYak – Street Chat)**
- ix. **Revenge Porn**

What Kids Should Do

- Don't respond
- Don't retaliate
- Talk to a trusted adult
- Save the evidence
- Block the bully
- Be civil
- Don't be a bully
- Be a friend, not a bystander

'Find A Voice'

What Should Adults Do?

- Listen & take child seriously
- Make sure child is and feels safe
- Don't overreact
- Encourage child not to retaliate
- Gather facts & save the evidence
- Get the child to help solve the problem
- Teach self-esteem & resilience
- Bring in school officials if there is a "nexus" with school
- Encourage child to reach out to friends
- **Encourage Courage:** "Be a friend, not a bystander"



What are the risks?

Sexy Selfie (Self Generated Images)

- I. Sending rude / explicit photos via email, social media, Apps and mobiles.
- II. Sending videos or exposing themselves on webcam
- III. Once they have been sent they can be put online or shared with anybody.
- IV. It is against the law if you have an explicit photo of someone under the age of 18 even if they are not 18 themselves. It does not matter if they are a boyfriend or girlfriend.



Sexy Selfie

iPhone – Android ?????

Why do kids/young adults send 'sexy selfies'?

Teen "romance" – expression of shared intimacy with partner



- Flirting / Prank
- Showing off (party behaviour)
- Impulsive risk-taking
- Peer pressure
- Revenge
- Bullying or intimidation
- Blackmail

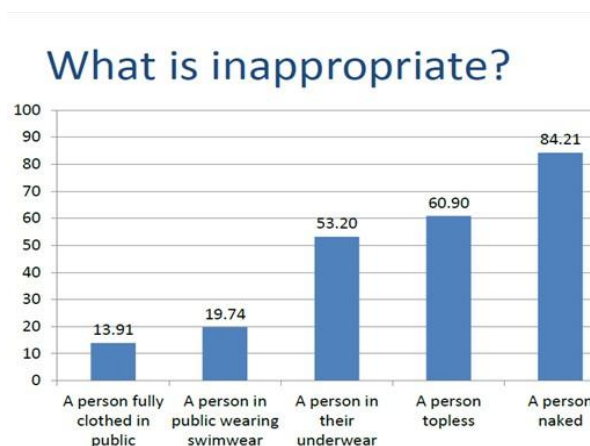
'Coz they Can'

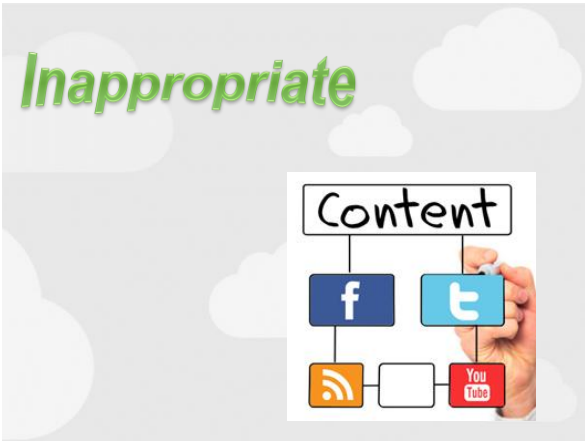
*"So take a dirty picture for me,
Take a dirty picture
Just take a dirty picture for me
Take a dirty picture"*

*From Taio Cruz song
No 6 in the UK charts
April 2010.*

Sexting (Sexy Selfie) Research

- Analysis responses from 30 UK schools, years 7-9, 1,150 students (boys & girls) in total.
- Asked questions regarding attitudes toward and behaviours around sexting, taking & receiving images.
- Questioned as to what they believe would be construed as Inappropriate







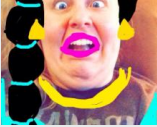


Why employers disregarded candidates?

Posted provocative inappropriate photo



53%



Why employers disregarded candidates?

Posted content drinking/using drugs

44%



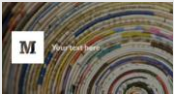
Your Digital Tattoo

It's About Having a Good Digital Tattoo

A online reputation is better than none at all

One of the best ways to bury embarrassing search results is to create with good ones.

OWN YOUR POST



With the rise of social media, many colleges and future employers have turned to it to find out more about their applicants.

Here are some tips to use with your children to protect their online reputation.



Allow it



By allowing your child to engage in social media at an earlier age, you are giving them an increased potential at understanding its appropriate use. Start the account together and decide what information should be posted. Go over some ground rules on what they are and are not allowed to post and what is deemed appropriate. Gradually allow your student to use social media more independently as they gain more Responsibility..



Monitor it

Check what your child / student is posting. If your child / student is posting about something that makes you question whether or not it's appropriate, it most likely isn't and imagine what others, i.e. a college admissions officer or potential employer, would think if they saw it. Watch the types of comments your child leaves on others' posts. Are they being respectful of themselves and others? Also, monitor the original content of the posts your child is liking or commenting on. Are their "likes" indicative of what they enjoy? Commenting or liking inappropriate content should be avoided.

Watch who they connect with



Anything or anyone connected to your child / student can be found. Monitor the photos and posts your child is tagged in. Who they are friends with online can affect the way others view your child. Also, check who and what they are following. Their interests can significantly influence their image.



Clean it up

Like a 'childs room', after a while a person's social media page can become cluttered and have some questionable choices. Just because something was posted two years ago, doesn't mean someone won't look at. Sift through older content on social media on occasion and clean up anything unnecessary. While everything posted on the internet is technically permanent, it can be beneficial to delete anything that raises question.

**Build a positive digital footprint
(to create a clean online reputation)**

The quickest way to check a student's digital footprint is through Google or other search engines. What amount of Information can be found? Is there nothing? Is there too much? It's getting to the point when nothing found on a student online can be hurtful, i.e. do they exist? But so can having too much. Teach your child / student how to effectively use social media to showcase his/her talents and potential. A positive digital footprint will enhance college and scholarship applications, or supplement a resume when your child is applying for a

STAYING SAFE ONLINE

Guard Your Information / Photos

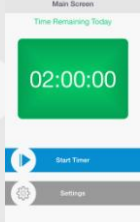
- Address
- Phone number
- School
- City
- Sports teams
- Parent's workplace
- Passwords
- SELFIES



STAYING SAFE ONLINE

Limit Time Online

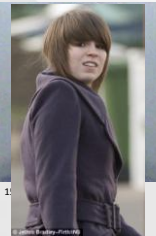
- Unplug and play
- Log Out v Shut Down
- Set Good Examples
- Contracts / Promises
- Take time for family
- Face-to-face time with friends
- No substitute for real exercise and sports
- Try the 2 Hour Challenge or even Week



STAYING SAFE ONLINE

Friend or Foe?

- Friends of Friends are 'Strangers'
- Seeing is not believing
- Games Require Oponents
- Random Play
- Turn off Wifi / 3G to Test Online Interaction
- Never schedule offline meeting with "online only" friends
- Tell your parents if anyone tries to meet with you offline



Online Contacts are Not Contacts – Online Friends are Not Friends they are
Unknown Internet Users

STAYING SAFE ONLINE

Communicate

- Don't bottle it up
- Ok to ask questions
- Stay away from "adults only" or 18+ sections of the Internet
- Tell your parents/carers about anything that makes you feel uncomfortable – sad –worried- frightened
- Educate parents/carers on Apps & Sites
- Be A Friend Not a Bystander
- FIND A VOICE

STAYING SAFE ONLINE

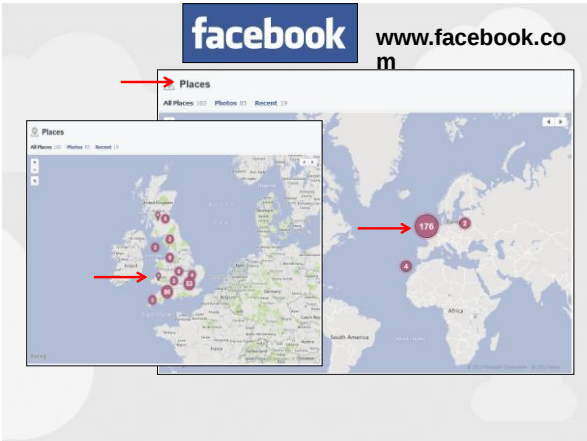
Webcam Safety

- Avoid File Sharing Systems – Putlocker / Bit Torrents
- Never do random chat
- Only chat with family and friends
- Never do anything on a webcam you wouldn't want up on this screen
- Think before uploading video responses
- Use Anti Virus / Adware / Malware / Spyware – or even cover up webcam

STAYING SAFE ONLINE

Time and a Place

- Carefully consider whether to use geolocation on social networks/games
- Never check in at school, church, or any place you visit regularly
- Check privacy settings
- Ask parents for permission before using any geolocation
- TURN OFF LOCATION SERVICES
- GPS should be only switched on when required
- GPS can locate users via data



Teamwork

- Get Involved
- Help each other
- Communicate
- Cooperate
- Know when to unplug
- TURN ON PRIVACY SETTINGS
- TURN OFF GMAIL SYNC
- TURN ON GPS WHEN REQUIRED
- MAKING THE RIGHT CHOICE

STRATEGIES



Thank you!

Jonathan Taylor

E-mail: besafeonline@ymail.com
Web Site : www.besafe-online.co.uk

 @Besafe_Online