


Riverside Online Safety Workshop (Parents)

Online Safety: Safeguarding Measures to Protect Your Child Online

Taking Care of Yourself 'Online'
Making The Social Use of the Internet 'Safer'
Through Understanding and Education


'A Little About Me'

Metropolitan Police 30 years
15 Years Child Protection Investigations
10 years Undercover Online Detective
MSc Criminal Psychology
ERA – Academy of Law, Trier

The Cycle to Reduce Risk


Daughters **Digital Tattoo**

Since 2009
Delivering Online Safety Training & Workshops for;
Schools (UK & International)
Foster Care Companies
University Guest Lecturer

Online Life Checked - Vetted



Bentley & Bruno



1



Online Safety Workshop Parents

What is Covered Tonight

- Online Exploitation
- Devices / Games / Social Media & Ages
- Online Competence / Resilience
- Grooming / Gaming / Bullying / SGI's
- GPS Issues
- Art Int / VR / Aug Reality
- Screen Time
- Digital Footprint / Digital Tattoo
- Advice & Resources

'Making the Right Choice to Stay Safe'



Online Safety 4 Schools
Online Safety 4 Schools

'Youth is Wasted on the Young'
'Wisdom is wasted on the Old'

Prevent Risks and Avoid Online Dangers

How ?

- Protection** → 
- Detection** → 
- Disruption** → 

Education

- Schools
- Students
- Staff / DSL's / Governors
- Parents
- Trusted Adults
- Carers
- Charities
- Professionals

Legislation

- Grooming
- Sextortion
- Cyberflashing
- Deep Fake Images???????
- (UK) Sexual Offences Act
- (UK) Online Safety Act
- (UK) Criminal Justice Bill
- (US) Childrens Online Privacy Protection Rule

Online Competence v Online Resilience

Options Open to Victims

- Forgive
- Forget
- Report
- Deal with Abuse & Offenders

3



Educational Tech

Pre - Internet



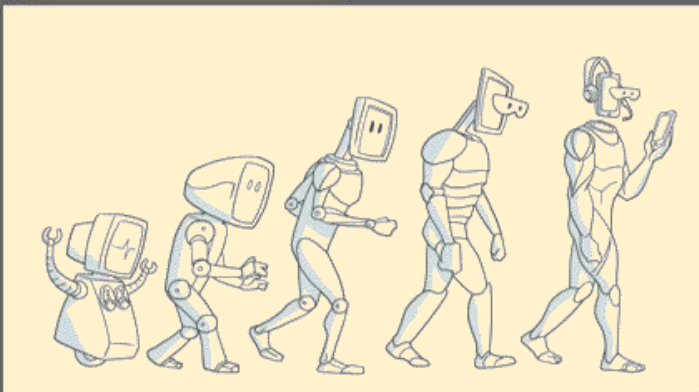
Current Internet

- Google Bard
- ERNIE
- YOU chat
- GPT-4
- Character.AI
- Socratic
- OpenAI
- Bing

Social Internet

- Devices
- Social Media
- Online Gaming
- Direct Messaging
- Gaming Communities

- 75% of people believe 6-12 year olds are at major or significant risk of sexual abuse in VR immersive spaces
- 80% of people believe 13-16 year olds are at major or significant risk of sexual abuse in VR immersive spaces



So....Best Why to Stay Safe?



Marcus Smith

or

Car crash



Falling off a Bike

How Could You 100% Guarantee this will never happen

1. Don't Play Rugby

1. Don't Drive a Car

1. Don't Ride a Bike

So.....

How Could You 100% Guarantee no 'Online Abuse' ?

Never Use a Device or SM / Games etc..... but is this realistic ?



Online Exploitation – 'via'

Social Media – Gaming - Gaming Communities - Direct Messaging

Sexual / Psychological Grooming

Online Gaming Issues

Online Bullying

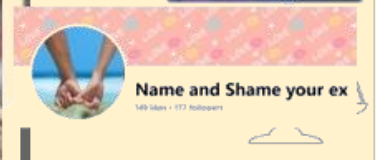
Self-Generated Images Inappropriate Images

Cyber Flashing / Technology Issues

Screen Time / Well Being

Child on Child Abuse

Digital Tattoo Damage



Adult Online Hate, Harassment and Abuse: A rapid evidence assessment

A review of existing evidence on online harassment (including cyberbullying and trolling), revenge pornograph and image-based abuse, and hate crime. The review highlights patterns of abuse based on age, sexual orientation, race and religion.



What are the Possible 'Online' Dangers

Stranger Danger

Online Bullying

Images

Friend on Friend

Digital Tattoo

Why?
Behaviour
 No Device / App / Game / DM / Website is created
 dangerous 'We All Have a Choice'

Hacking

Well Being

Phishing

Emotional Dangers

Physical Dangers

Online Gaming

Gaming Communities

Direct Messaging

Art Int

7



Current Devices

Current Social Media

Current Games

Current Gaming Communities

Current DM's

New Tech

Current Online Challenges

Reality

5 & 6 year olds 20%

7 & 8 year olds 40%

9 - 11 year olds 60%

12 & Up 90 - 100%

Smart Phone is go to device (STREAMING)

Most Installed Apps (Image / Video / DM Apps)

What age should a child 'have their own 'Smart Phone'.

1. Ages 0 – 10

Age 0 – 10 – No Phone – No Need.
Unless there are 'care', 'safety' or 'custody' issues there is no need for Under 10's to have mobile phones.

2. Age 10 - 13

Age 10 - 13 – Mobile Contact with children may now be necessary so a 'Brick Type' Phone, that allows for SMS, text messaging and managed phone calls is a possibility. This type of phone is required for parental contact with son/daughter and not required for 'Internet' or 'Selfies' or Apps or Games.

3. Age 13

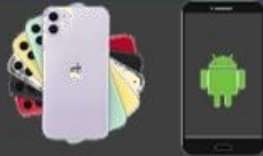
Age 13 – To allow no feeling of exclusion, parents may consider a smart phone that has limited Internet access, limited contact lists. Parents should consider a signed Smart Phone Contract to set boundaries which in turn encourage 'appropriate behaviour'. Parents must install Google Family Link (Android) & Family Sharing (Apple), to control & prevent installing of Apps. See Note Below.

4. Age 13-14

Age 13 – 14 – Consider a Smartphone (without Social Media installed), use Google Family Link (Android) & Family Sharing (Apple). Parents control the installation of Messaging, Gaming and Social Media Apps. See Note Below.

5. Age 14 - 16

Age 15 – Smartphones with Social Media & Gaming Apps installed can be allowed – parents should now continue to monitor their child's online activity, and be a part of their child's Social Media, Gaming and Messaging life. See Note Below.



'Making the Right Choice to Stay Safe'

Online Safety 4 Schools

Online Safety 4 Schools



Reality

5 & 6 year olds 20%

7 & 8 year olds 40%

9 – 11 year olds 60%

12 & Up 90 - 100%

Smart Phone is go to device

(STREAMING)

Most Installed Apps

(Image / Video / DM Apps)

Technological Issues with Mobile Phones:

Mobile phones are the 'go to' device for posting & scrolling Instagram, Snapchat, & Tik Tok. Parents must remember that if Internet Connectivity (WiFi or 4g) is available & 'On' then any picture taken will be uploaded to either i Cloud or Google Cloud (Digital Tattoo).

If posts are made to Instagram with GPS 'on' then free software allows for 'strangers' to locate users & their posting locations (Home), so GPS must be switched off when at 'Home' & only used by Under 17's when requested by Parents/Carers.



Online Safety is about Behaving Appropriately

Top Tips for Parents / Carers



9

'Making the Right Choice to Stay Safe'

Introducing the Online Safety Spectrum

Acceptable

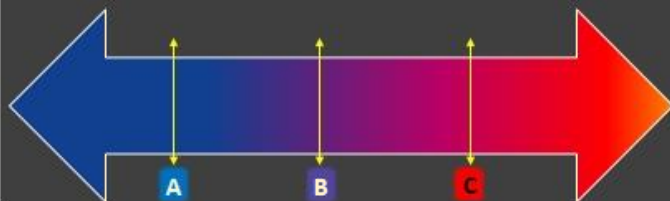
Unacceptable

Appropriate

Inappropriate

Legal

Illegal



CHILDREN'S ONLINE BEHAVIOUR AND SAFETY

- 'Staying Safe Online' requires 'Acceptable Behaviour' this very often requires difficult decisions for 'young users'
- Consider where online users should be & where children are and where you would place yourself.

Where would you put yourself on the spectrum

What about 6- to 18-year-old students

Online Competence when using Social Media , Online Games , Gaming Communities & Direct Messaging

Intended Competence

- Deliberate Appropriate Online Behaviour

Unintended Competence

- Accidental Appropriate Online Behaviour

Intended Incompetence

- Deliberate Inappropriate Online Behaviour

Unintended Incompetence

- **Accidental Inappropriate Online Behaviour**

Online Competence is the ability to use a device that has access to the Internet, with knowledge, and skill that indicates expertise and understanding of usage.

Who Decides ?

Competency

Many Parents decide 'competency' by supplying their child with a device perhaps due to pressure (gifts) or mobile phone required as child now at school –

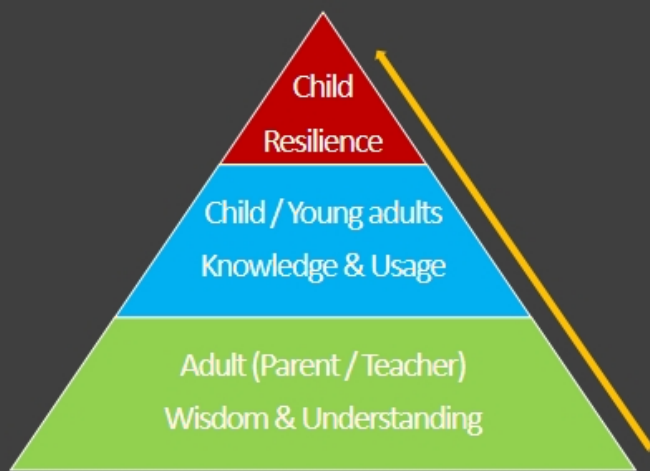
NO CONSIDERATION IS GIVEN TO COMPETENCY

Ignoring Age Restrictions
 Not Asking Permission
 Not Taking Regular Breaks
 Random Play
 Random Requests
 Random Notification
 PMOYS / Peer Pressure
 Stranger Danger
 Affluent neglect / No Supervision

Recognising, Understanding & Acting



Resilience
Effective Online Resilience will only be created through Parental Involvement, and advice and Contribution from other Trusted Adults (Teachers etc)



Digital skills and competence, and digital and online learning

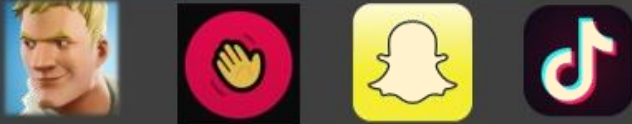
Online resilience is the ability to bounce back from difficult times online over time

How ?
 True Friend & Family Support
 Regular Breaks Prevents poor Judgement
 Treat people How you wish to be Treated
 Happy to Talk
 Let Parents / Carers Into Online Life

3

Sexual / Psychological Stranger Danger

Online Predators contact their victims using four main ways:



Social Media / Gaming Apps & Websites / Chat Rooms / Video Game Communities

Predators will use these same Sites / Apps / Video Game Communities, to gain access to possible victims.

There is little need to create a 'friendship / rapport stage' with the victim as the victim has already shared personal information

Children communicate and interact with other users or are prepared to add other online users to gain 'online credibility' by having many online contacts.

SO ONLINE PREDATORS TEND TO HIDE IN PLAIN SIGHT

What Parents must 'question' about Apps being used

What age does the App require users to be?

Does the App have direct messaging or chat capabilities?

Are users 'Live Streaming'?

Does the App have any parental controls or filters available?

Does the App use location tracking? (GPS - Location Services)



Online Predators - The Next Stage:

Once the predator has seized the opportunity gained access to the victim, and has begun the online interaction



the predator will invite the victim to a 1:1 interaction using a free direct messaging app available (Closed Groups)



WhatsApp Kik Messenger We Chat Messenger Skype Zoom



13



Positive Effects of Online Games on Children & Young Adults

Improves cognitive functions

Hand and eye function

Precision and decision making

Improve teamwork

perseverance, accuracy, and logic

Experimenting with aspects of individual identity

Improving problem-solving skills

Math and reading skills

Harmful impact on health

Pressure & Stress

Negative Effects of Online Games on Children & Young Adults

Addiction

Aggressive behaviour

Isolation from society (Self Inflicted)

NEGATIVE EFFECTS

Isolation from society (Enforced)

Failure

Screen Time (POOR)

Concentration & Memory

Online Bullying 'No Borders'

Cyberbullying drives 13-year-old to attempted suicide with insecticide in Vietnam



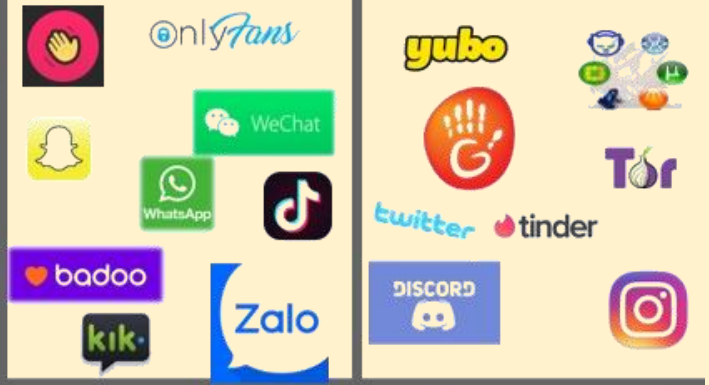
A 13-year-old girl from Vietnam's Mekong Delta has survived after attempting to commit suicide by drinking insecticide, as she had been cyberbullied by her classmates

Pressure & Stress

It was Just Banter

Throw Away Comments

Didn't Mean it



Physical

Verbal

Emotional

Cyber

Hitting, kicking, pushing, taking or hiding things

Name calling, teasing, insulting, threats, gossiping

Looks, Exclusion, leaving out of groups, Ignoring- (SnapMaps, WhatsApp Groups)

WhatsApp, Discord, Snapchat, Instagram, Steam/Twitch

15



'Making the Right Choice to be Safer'

Inappropriate Selfie



The term 'Inappropriate Selfie / Image' is used to describe the streaming sending and receiving of photos, messages and video clips, on platforms or text, email. It's increasingly done by young people who send images and messages to their friends, partners, or even strangers they meet online.



If you would not want your parents or grandparents to see how you look then you shouldn't be streaming, taking or sharing.

An Inappropriate Image Can Affect your Future



But - What is an Inappropriate Selfie (Image)?



Online Challenges / Incitement / Self Harm / Self Esteem

Anonymous People Setting Up Challenges on 'Social Media' - Only Completed when Posted on Social Media &/or You Tube

- Blue Whale Challenge – V Kontakte → 
- 'The Tide Pod Challenge' → 
- The Snorting Challenge → 
- The Deodorant Challenge → 
- Momo Challenge → 
- Shell On Challenge → 
- Tik Tok Silhouette Challenge → 
- Tik Tok Skull Breaker Challenge → 
- Tik Tok Black Out Challenge → 
- Tik Tok Chroming Challenge → 
- Tik Tok Cinnamon Challenge → 
- Tik Tok Throw It in the Air Challenge → 
- Tik Tok Benadryl Challenge → 
- Tik Tok Monthly Challenges → 

Motivational Challenges

Ice Bucket / Fitness etc

Neutral Challenges

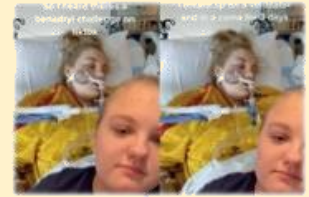
Dance / Fruit etc

Dangerous Challenges

All Prey on the Vulnerable

Boy, 13, dies after trying dangerous TikTok 'Benadryl Challenge'

Warning after schoolboy almost dies from swallowing magnets for TikTok challenge



Whilst all these challenges are physical not technological, without the use of technology (mobile phones / tablets etc), the message could not be spread, therefore the **online validation sought**, the **online badge of honour** received, and the **online motivation and justification** for behaving this way would not be warranted or 'go viral'.

Online Pressure
Child on Child Pressure

Pressure & Stress

TikTok has grown in popularity, particularly among young people and teenagers. Its trends have progressed beyond simple dance moves, jokes, tracks, combined video formats, and WORSE, into toxic trends that can take the lives of your children.

17



Online Image Financial Extortion

Online Image Financial Extortion involves people being forced into paying money or meeting another financial demand, after an offender has threatened to release inappropriate photos of them. This could be a real photo taken by the victim, or a fake image created of them by the offender.



Global **offending** reported to (NCMEC) more than **doubled in 2023**, rising to 26,718 compared to 10,731 the year before.

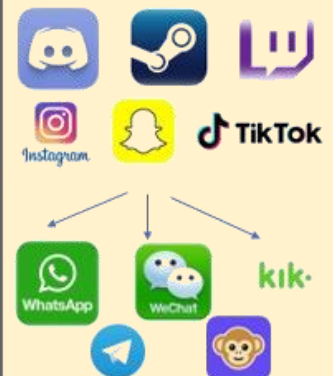
All age groups and genders are being targeted, but a large proportion of cases have involved male victims aged between 14-18.

91% of victims in UK IWF in 2023 were **male**.

These crimes can be perpetrated by organised crime groups based overseas, predominantly in some **West African** countries, but some are also known to be located in **South East Asia**.

Offenders are motivated by making money quickly, rather than by sexual gratification, & blackmailing their victim in under an hour.

Blackmailed after sharing an image or video, or the offender sharing hacked or digitally manipulated/AI-generated images of the child or young person and making the threat of sharing them wider



Online Image Financial Extortion (How)

Contacted by Online Stranger pretending to similar age

Contacted by Friends Hacked Account

Inappropriate Explicit Communication

Manipulated into taking inappropriate photos or videos

Told they've been hacked and the offender has access to their images, personal information and

BLACKMAILED

Gift Cards

Keeping Children Safe in the Digital World

Viewing Inappropriate Images

Very Easy to Access (All Platforms)

Electronic Verification of Age (Pornhub)

Experimentation (Criminalisation of Children ?)

Normalisation of inappropriate activity ?

'Perfect Body' – self-esteem issues

Viewing Extreme Activity / Degrading Objectifying People)

Age Equivalent viewing maybe a criminal offence

Is it Viewing or Collecting

Parental Controls, Restrictions & Communication

Is This an Issue – Remember

- By age nine, 10% had seen inappropriate images
- 27% had seen it by age 11
- Children who see inappropriate images for the first time at age 11 or younger are likely to have lower self-esteem as young adults
- 70% of kids ages 8-18 have accidentally encountered online inappropriate images, very often by entering an innocent search term while doing their homework
- 31% of kids ages 12-18 have lied about their age in order to access a website
- 90% of children ages 8-16 have seen online inappropriate images.

VERY HIGH PERCENTAGE OF CHILDREN HAVE NOT VIEWED

It is Not Unusual for Young Adults and Young Children to have viewed Online inappropriate images

Innocent Curiosity / Accidental Viewing

Ease of Access / Peer Pressure

NO MENTAL HEALTH ISSUES

19



Receiving Images without Request



Cyber Flashing...



Is there any Difference...

Pressure & Stress



A 2020 study found that three-quarters (76 %) of teenage girls between the ages of 12 and 18 have been exposed to Cyber Flashing. More recently a 2022 study found that more than a fifth of girls and young women aged between 13 and 21 in the UK have been Cyber Flashed in 2021.

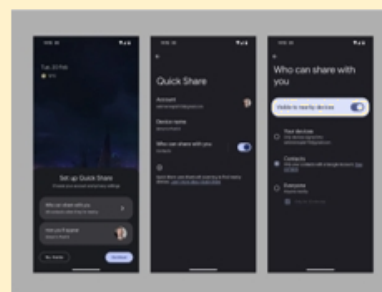
Fear Of Missing Out
FOMO

Somebody who sends an image that you did not request or ask for & the picture makes you feel awkward, frightened, embarrassed is committing an offence - **SO**

ONLY SEND / EXCHANGE / RECEIVE IMAGES FROM FRIENDS YOU TRUST

ONLY USE BLUETOOTH & AIRDROP WITH FRIENDS YOU TRUST AND FOR PICTURES YOU HAVE ASKED FOR

DE-PERSONALISE THE IPHONE / IPAD



5

ACTION MUST BE —REPORT — SUPPORT —

Excessive Device Use + Screen Time Tiredness Creates Mistakes



Tiredness can Create Mistakes



- live opponents friends and strangers risk – grooming and bullying
- online purchases (loot box) (V Bucks) risk gambling and debt (parents)
- unsuitable imagery risk (fright and aggressive behaviour)

Online Gaming – The Risks & Dangers

Playing games against friends and strangers.

What Are the Mistakes ?

6

- Saying Things, You Don't Mean*
- Adding People You Don't Know*
- Chatting With People You Don't Know*
- Visiting Using Apps / Sites You Wouldn't Normally Use*



Augmented Reality as a means for Harassment and Harm

Different types of harm identified through the use of Augmented Reality

Pokémon GO Teams Are Becoming Gangs, Complete With Vandalism and Bullying



Virtual objects intercept the real world in real-time.

VR can be described as a simulated visual experience that can be similar or different from your surrounding environment.



Meta has started forcing "space sense" to be on

Virtual Reality - What are the Possible 'Online' Benefits Dangers

Why? Behaviour

- Experiencing physical injury
- Negative impact on mental wellbeing
- Experiencing unwanted contact
- Encountering harmful content
- Oversharing private information



EDUCATION

Escapism

Exploring Different Environments

Connecting with OTHERS

Exploring Identity

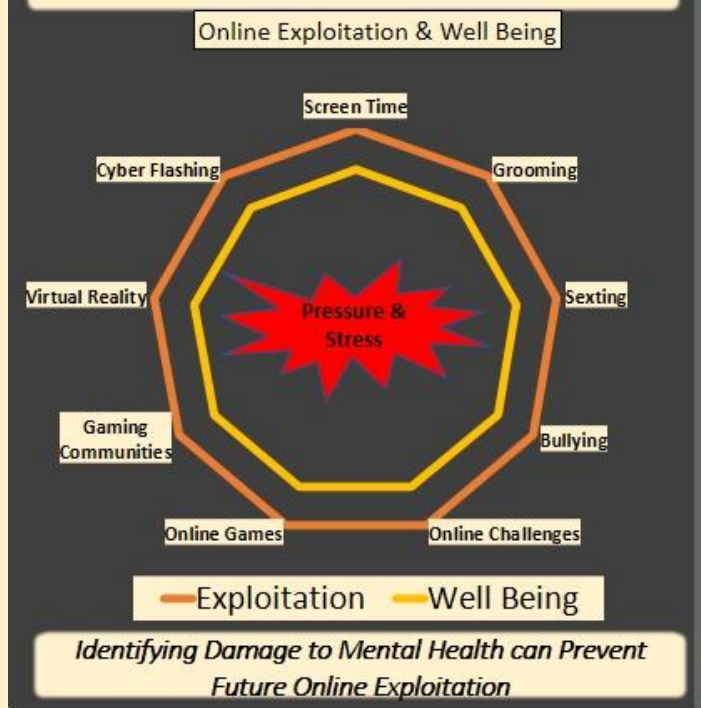
VR multiuser spaces provide opportunities for offenders to commit child inappropriate abuse and exploitation against a child.

'Phantom touch'* can mean that victims of VR abuse experience the physical sensation of being touched without their consent.

VR multiuser spaces can desensitise offenders with avatar disguise and anonymity 'normalising' their abusive behaviour.



Online Safety in 2024 and Beyond



Changes in temperament/ depression / mood swings

Disengagement from education

Secrecy

Risky Behaviour

Sexual health concerns; sexually transmitted infections / pregnancy

Older boyfriend / girlfriend / friends

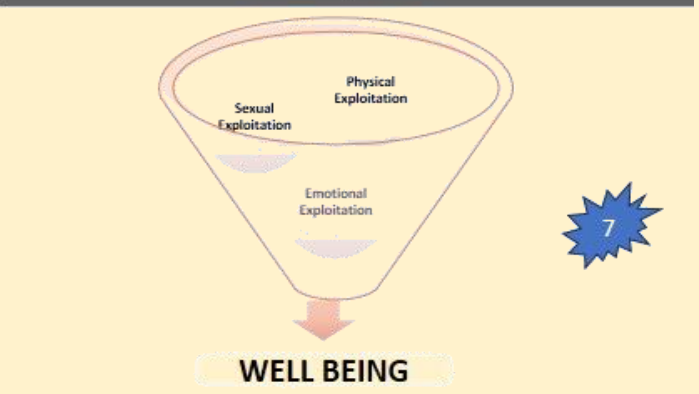
Association with other young people involved in exploitation

Inappropriate use of Social media / Gaming

Drug and alcohol misuse

Exclusion

Going missing or running away from home



Online Safety isn't Just about Stranger Danger etc Things have 'Moved On'

Inappropriate – Illegal – Unacceptable
Social Media – Gaming – DM – Gaming Community Comments

Friend on Friend Abuse

Child on Child Abuse

Group on Group Abuse

Signs could be 'physical' or 'emotional' or 'behavioural' leading to the child appearing withdrawn, frightened, the signs may also be physical (swelling)

Disclosure – is always very difficult for any victim of online abuse, this takes resilience, confidence, and immense strength, not that common in some young adults.

Barriers to a Not Reporting

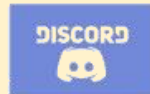
Fear of teachers not keeping secret Fear of getting into trouble

Fear of losing friends – name calling

Fear of not being believed Fear of parents finding out

Fear of being thought of as a snitch

Not making a 'fuss', Blame Themselves



Online Safety 4 Schools

Online Safety 4 Schools

Pressure & Stress

REPORT & TELL

TRUE FRIENDS
SUPPORT
EACH OTHER

Reassurance
Understanding
Communication

25



Keeping Children Safe in the Digital World

What is an Online Identity ?
Can it affect your Future ?

From our **gender, ethnicity and age** to our **experiences and behaviour**, every aspect of our life can form part of our identity.

We can have many **different identities** which come together to form who we are, and we can create, adapt and change our identity when we choose. **'Online Profiles'**



Online Safety 4 Schools

Online Safety 4 Schools



Social Media & Online Safety Consultant

Your Digital Tattoo Online Identity



Online Safety 4 Schools

Online Safety 4 Schools



8

Take It Down.
Having notes online is scary, but there is hope to get it taken down.

This content is only available on our membership website. Contact your school's IT or security departments and online safety officers for more info.



Your Digital Tattoo Online Identity



27



Children Should Ask Permission – Encourage Children to ask and 'Get Involved'

"Is it okay if ...?"

"Please can I ...?"

"Would you like to ...?"

"What should I do if ...?"

'I Play Fortnite/Roblox/Minecraft'
'Play Games on my Smartphone'
'Use my Nintendo Switch/PSS/Xbox'

'Making the Right Choice to Stay Safe'



'Play for another 20 Minutes' 'Add a True Friend from School'
'Play after I have supper.'

16

'Play the Game with me'
'Watch how I get a high score'
'See who my contacts are'

'I receive Requests or Notifications from people I do not know'
'I get a pop-up offering V Bucks'
'I get a friend Request'



Online Safety 4 Schools

Online Safety 4 Schools



Online Safety Workshop Parents

What were the 'Tips'

- 1 Smart Phone –Family Sharing/Google Fam Link/GPS/Selfies
- 2 Competence decided by Parents – So Discuss
- 3 Create Resilience by Corridor of Communication
- 4 Question Apps
- 5 Cyber Flashing – Friends you Trust – De-Personalise
- 6 Reduce Screen Time / Technology is a Privilege
- 7 Pressure & Stress / Well Being B4 Exploitation
- 8 Online Identity – Google / FaceCheck ID

Online Safety 4 Schools

Online Safety 4 Schools



'Making the Right Choice to Stay Safe'

**'Youth is Wasted on the Young
'Wisdom is wasted on the Old'**

9 - 14

15

16

Resources

Software (Free to £'s)

Four (4) Questions

Online Safety Guidance for Parents – Carers & Trusted Adults

What to 'Take Away' (Overall Awareness)

- Online Competence defines Appropriate Age
- Online Gaming has its Positive Side but be aware of the Negatives as well
- Online Predators Hide in Plain sight
- Online Bullying occurs in 'Closed Groups'
- Monitored Screen Time can prevent Online Exploitation
- Student on Student Abuse is far for likely than Stranger Danger

Screen Time


Online Challenges

Best Practice

Responsibilities

Child on Child

Digital Tattoo



Jonathan Taylor MSc

www.onlinesafety4schools.co.uk
onlinesafety4schools@gmail.com