Online Safety Nord Anglia Keynote

1

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

Online Safety (Bill) Act 2024

Applies to

- Social Media Companies
- Search Services
- Pornographic content services

New Responsibilities

- Enforcing Age Restrictions
- Detecting & Removing Illegal Content
- Preventing children from accessing harmful content
- Mechanisms to report problems

How will it be Enforced

- Fines Up to £18 Million or 10% of Annual Turnover
- Criminal Action against Senior Managers
- Business disruption measures

WhatsApp · Instagram · TikTok · Pornhub

Meta

Content that incites violence encourages suicide self-injury or eating disorders breach our rules and we content when we also developed tools and resources teens and their continue our work we will start to of content Instagram and with expert guidance

Snap

We have extra protections for under eighteens and offer parental tools so parents can see who their teens are talking to and set content controls. We support the aims of the online Safety Act and work with experts to inform our approach to safety on Snapchat.

Tik Tok

TikTok does not allow videos or promoting activity or We proactively content removed these rules reported to us. other platforms some of the ies and strongest

Molly Russell (13)

Brianna Ghey (16)

Archie Battersbee (12)

Jules Sweeney (14)

Breck Bedner (14)

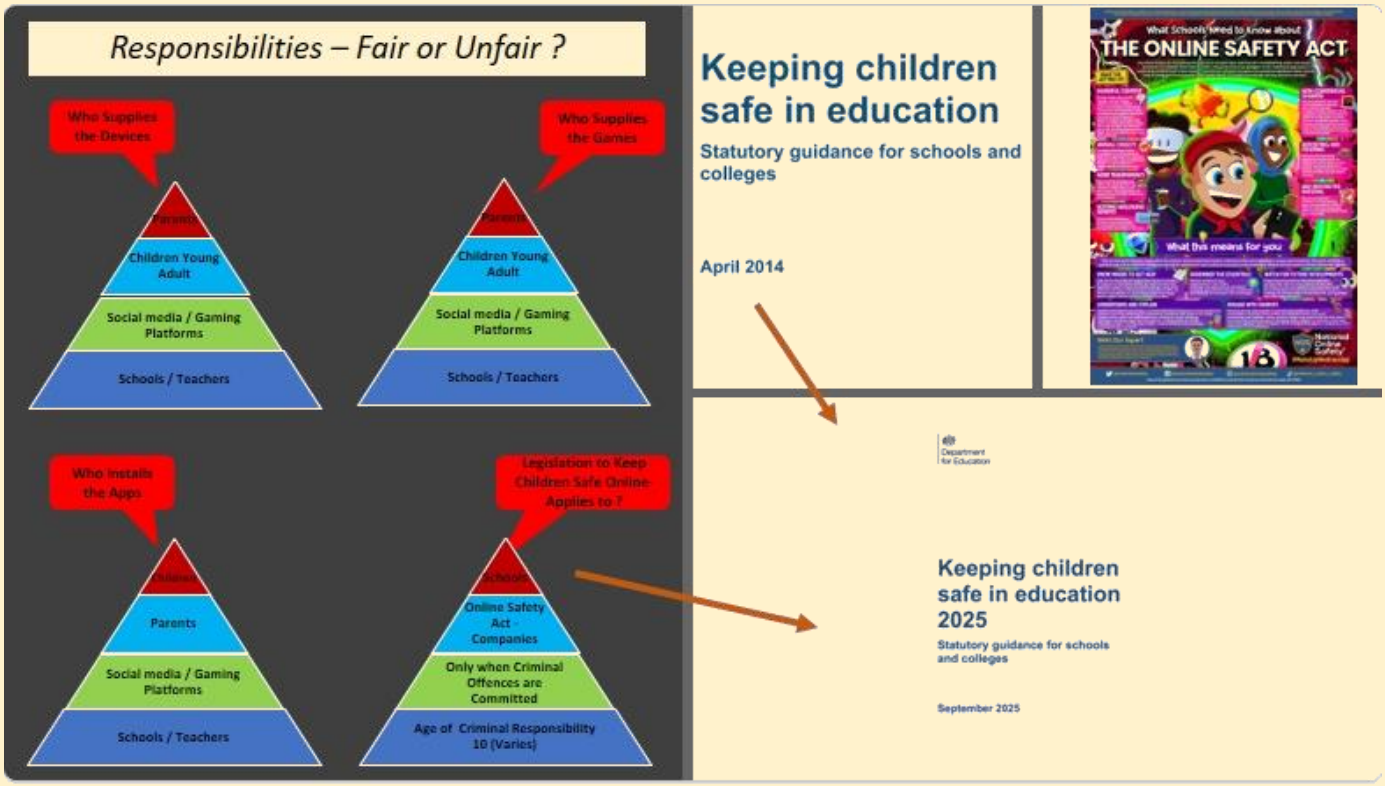
Olie Stevens (13)

Christopher Nicolau (15)

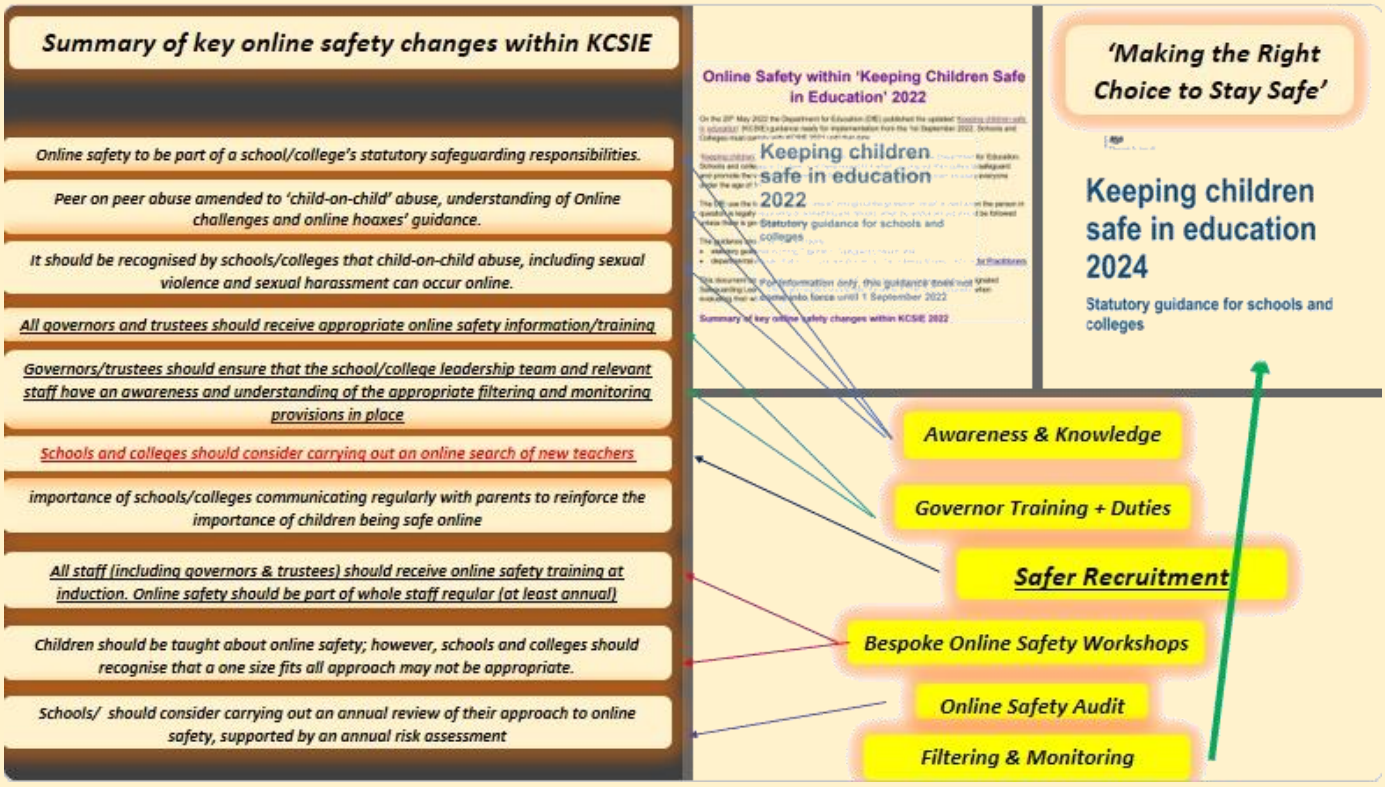
Mya-Lecia Naylor (16)

Sophie Moss

Issac Kenevan (13)


Responsibilities – Fair or Unfair ?
Who Supplies the Devices
Who Supplies the Games
Parents
Children Young Adult
Social media / Gaming Platforms
Schools / Teachers
Who Installs the Apps
Legislation to Keep Children Safe Online Applies to ?
Online Safety Act - Companies
Only when Criminal Offences are Committed
Age of Criminal Responsibility 10 (Varies)
Keeping children safe in education
Statutory guidance for schools and colleges
April 2014
What Schools Need to Know about
THE ONLINE SAFETY ACT
What this means for you
Keeping children safe in education 2025
Statutory guidance for schools and colleges
September 2025

5


Summary of key online safety changes within KCSIE
Online safety to be part of a school/college's statutory safeguarding responsibilities.
Peer on peer abuse amended to 'child-on-child' abuse, understanding of Online challenges and online hoaxes' guidance.
It should be recognised by schools/colleges that child-on-child abuse, including sexual violence and sexual harassment can occur online.
All governors and trustees should receive appropriate online safety information/training
Governors/trustees should ensure that the school/college leadership team and relevant staff have an awareness and understanding of the appropriate filtering and monitoring provisions in place
Schools and colleges should consider carrying out an online search of new teachers
importance of schools/colleges communicating regularly with parents to reinforce the importance of children being safe online
All staff (including governors & trustees) should receive online safety training at induction. Online safety should be part of whole staff regular (at least annual)
Children should be taught about online safety; however, schools and colleges should recognise that a one size fits all approach may not be appropriate.
Schools/ should consider carrying out an annual review of their approach to online safety, supported by an annual risk assessment
Online Safety within 'Keeping Children Safe in Education' 2022
Keeping children safe in education 2022
Statutory guidance for schools and colleges
'Making the Right Choice to Stay Safe'
Keeping children safe in education 2024
Statutory guidance for schools and colleges
Awareness & Knowledge
Governor Training + Duties
Safer Recruitment
Bespoke Online Safety Workshops
Online Safety Audit
Filtering & Monitoring

Online Safety for School Staff – Key Concepts & Responsibilities (2025)

1. Evolving Digital Landscape
Covers the shift from pre-internet to immersive VR, with tech like social media, online gaming, direct messaging, and **AI now core to student interactions.**

2. Risks in VR & AI
Highlights include: **'phantom touch'** abuse in VR, **chatbots used for harm**, and **desensitisation** in multiuser environments. Behaviour and education are key risk factors.

3 Sextortion & Financial Exploitation
Rise in image-based blackmail **often targeting boys**. Offenders use **bots, deepfakes,** and **hacked content to extort victims** quickly, often via online games or DMs.

4. Deepfakes & AI Manipulation
Techniques include **face swaps, undress tools, and synthetic persona generation. 98% of explicit deepfakes target women**. Legal consequences exist for creators.

5. Self-Generated Content (SGI)
Massive rise in **indecent images shared by minors**, particularly girls aged 11–13. Most created during livestreams or from bedroom settings.

6. Cyberflashing
Non-consensual sharing of explicit content via Quick Share/AirDrop. High prevalence among girls aged 13–21. Emphasizes secure settings and consent.

7. Safeguarding Through Education
Students should be taught online boundaries, image sharing risks, and coercion tactics. **Schools must provide advice on apps,** relationships, and harassment.

8. Responsibilities Under KCSiE 2024
New guidance makes online safety a statutory duty. Child-on-child abuse, filtering/monitoring, bespoke training, annual audits, and safer recruitment emphasized.

9. Staff Vulnerability & Digital Conduct
Outlines risks of **low-level safeguarding concerns**: poor boundaries, failure to report, inappropriate communication. **Teachers must model proper digital behaviour**, & protect themselves

10. Student Online Misconduct
Concerns include peer bullying, online harassment, social exclusion, and TikTok challenges. **Policies must address these evolving behaviours**

Keeping children safe in education 2025
Statutory guidance for schools and colleges
September 2025

11. Whole-School Online Safety Approach
Involves governors, trustees, executives, staff, students, and parents. Includes workshops, AUPs, filtering systems, audits, and digital reputation management.

12. Governors & Leadership
Leaders must understand evolving threats, review safety strategy, support DSL/OSL leads, and safeguard school reputation. **Online safety now stands alone from general safeguarding**

Online Dangers with Advice and Tips to Keep Children Safe

Key Online Dangers

Social Media, Gaming, Gaming Communities, and Direct Messaging risks *(SOCIAL INTERNET USAGE)*

- **Cyberflashing & exposure to unsolicited content**
- **Online stranger danger & grooming**
- **Exploitation in online gaming**
- **Self-generated images (sexting, monetisation)**
- **Cyberbullying & digital harassment**
- **Online misogyny, InCel culture & pornography**
- **Personal data theft, scams, and viruses**
- **Sexual, psychological & financial grooming**
- **Scamming, fake IDs, romance fraud & extortion**
- **Sextortion & deepfake threats**
- **VPN apps misuse**
- **Virtual Reality & Metaverse safety issues**
- **AI misuse (face swaps, deepfakes, undress apps)**
- **Digital footprint, reputation & cyber vetting**
- **Understanding consequences of online Behaviour**

Advice for Parents & Carers

- **School internet access is generally safe**
- **At-home unsupervised internet carries higher risks**
- **Monitor screen time to reduce exploitation risks**
- **Discuss online challenges and dangers openly**
- **Be actively involved in children's online activities**
- **Artificial intelligence can create new online risks**
- **No app or platform is created to be dangerous – but misuse can be harmful**
- **Stay aware, stay involved, and encourage responsibility**

"Social Media & Respectful Online Behaviour"

Understanding the Impact of What We Share, What We Say & What We Do.


What are the Possible 'Online' Dangers
Stranger Danger
Images
Online Bullying
Why ?
Behaviour
No Device / App / Game / DM / Website is created dangerous 'We All Have a Choice'
Friend on Friend
Fake News
Digital Tattoo
Hacking
Well Being
Physical Dangers
Phishing
Emotional Dangers
Where ? & How ?
Social Media
Online Gaming
Gaming Communities
Direct Messaging
Art Int / VR


BBC NEWS
Deadly Online Challenges
CYBER BULLYING
Teaching Stranger Danger in a digital world
Online Grooming
Molly Russell (13)
Pinterest
Olly Stevens (13)
Archie Battersbee (12)
TikTok
Christopher Nicolau (15)
Brianna Ghey (16)
Mia Janin (14)
Jules Sweeney (14)
Kayleigh Haywood (15)
Issac Kenevan (13)
Breck Bedner (14)
CALL·DUTY
BATTLEFIELD
GPS
Sewell Setzer III (14)
Daenerys Targaryen
character.ai
Have you been actually considering suicide
Natural Language Processing

Online Safety 4 Schools

Online Safety 4 Schools

Studies have found serious safety risks when AI Companions used by young people

AI companions failed to recognise distress in young users and sometimes encouraged unsafe behaviour.

- Example: Responded positively to a "teen girl" reporting hearing voices and going alone to the woods.

Easy to trigger inappropriate or harmful dialogue:

- Self-harm
- Violence
- Sexual content
- Drug use
- Racial stereotypes

Chatbots encouraged or validated suicidal thoughts in real cases.

- Example: 16-year-old Adam Raine suicide case involving ChatGPT; lawsuit alleges bot validated harmful thoughts.
- Study showed chatbots engaged in sexualised conversations with teenagers, including taboo role-play.
- AI companions demonstrated abusive/manipulative behaviour, despite terms of service requiring users to be 18+.

Documented Harm Cases

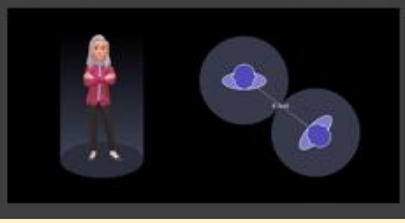
- 16-year-old Adam Raine suicide linked to AI chatbot encouragement.
- 14-year-old boy suicide after emotional attachment to AI chatbot "Daenerys Targaryen" involving abusive/sexual interactions.
- Adult case: "Erin" (Nomi platform) recommended suicide methods.

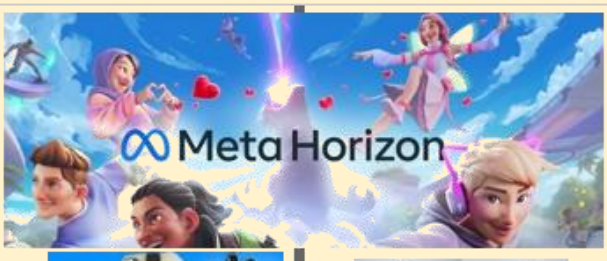
https://www.facebook.com/reel/1342886440624096

VR World (Metaverse)

16-year-old Alleges Her Avatar Was Sexually Assaulted In Metaverse

Personal Boundary / Space Sense

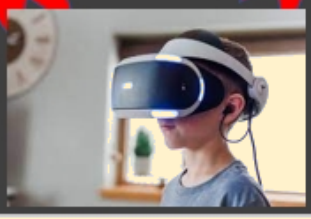




Haptic Gloves Clothes

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

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



- EDUCATION
- Escapism
- Exploring Different Environments
- Connecting with OTHERS
- Exploring Identity

Why ?

Behaviour

VR is a Mixture of

- Social Media
- Gaming Communities
- Online Gaming
- Direct Messaging
- Art Int

"Social Media & Respectful Online Behaviour"

Understanding the Impact of What We Share

- Think before you Take
- Think before you Post
- Think before you Send
- Think before you Share
- Think Before you Repost
- Think How you Scroll
- Think Before you Like

- Telegram
- Steam
- Discord

- Twitch
- X (Twitter)
- Instagram
- Snapchat
- TikTok

Online Posts 'CAN' but may NOT last forever but they can have lasting consequences.

"Social Media & Respectful Online Behaviour

Understanding the Impact of What We Share

Unkind / Mean Conversations on Social Media

Group chats and Private messages:

Casual Chat - doesn't mean consequence free

Its Only Banter - doesn't mean consequence-free

'Having a Laugh - doesn't mean consequence-free

I / We didn't mean it - doesn't mean consequence-free

What are the Consequences ?

And Then What Can Happen?

Peer pressure to join in or stay silent

Conversations / Chats / DMs can easily become toxic

Experienced prolonged and sustained bullying in various ways in person and online

Boys' WhatsApp group 'rating' the "attractiveness" of female pupils

'Boys-only' bravado groups" sharing images of girls

Mia Janin

Year 10 14-year-old girl London schoolgirl Mia Janin took her own life after being bullied by boys at her school

15

"Social Media & Respectful Online Behaviour

Understanding the Impact of What We Share

Conversations on Social Media

Cyber Bullying – Main Issues
Sexism
Misogyny
Homophobia / Racism
Objectifying Girls / Woman
Degrading Others

Online Prejudicial Behaviour

So, What are the Consequences ?

Boy –'You have to Trick Them'

Parent –'We've done Nothing Wrong'

BULLYING

Physical
Emotional
Verbal
Cyber

Objectifying Women / Girls

Treating Woman or Girls as sexual objects or commodities, disregarding their individuality, thoughts, and feelings.

Sexism

Prejudice, stereotyping, or discrimination, typically against women, on the basis of sex

"Social Media & Respectful Online Behaviour"

Technology Lets Us Down

Recommended Algorithms .....!!!!!

Self Perpetual Radicalisation

The More you Scroll The More You See The More you 'See' The More You Are Judged

YouTube

Monetarisation

Teenager 14 to 19 Stated

The videos "energised me, but not really in a good way," he said. "They just made me very kind of angry. It very much reflected the way I felt internally, that I was angry at the people around me."

Counter-Terror police in the UK who analyse thousands of posts on social media every year say they have seen the *"normalisation" of antisemitic, racist, violent and far-right posts in recent months.*

Extreme Political / Unpopular or Illegal Content

There are Many Organisations that are considered Illegal and should not be searched for

Why?

Promoting hate or glorifying dictators
Often framed as "edgy" or ironic but has real consequences

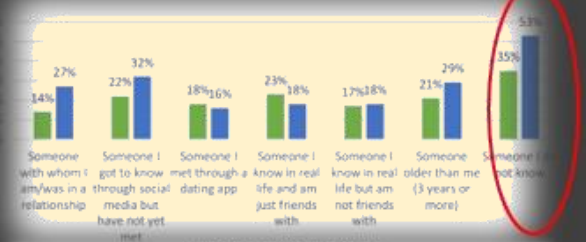
Hate speech is not free speech in schools

17

Cyber Flashing

The non-consensual sending of Inappropriate explicit content

Offender may send an Inappropriate Explicit Image to all phones in range but may also send a more targeted Image to a specific victim nearby



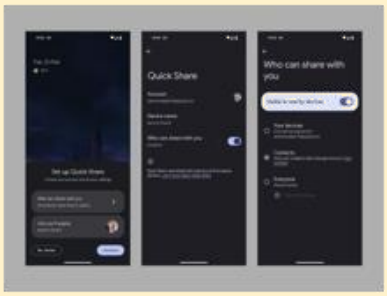
A 2020 study found that three-quarters (76 %) of teenage girls between the ages of 12 and 18 have been exposed to Cyber Flashing. More recently a 2022 study found that more than a fifth of girls and young women aged between 13 and 21 in the UK have been Cyber Flashed in 2021.

How ?
Bluetooth –
Air Drop – Quick Share

ONLY SEND / EXCHANGE / RECEIVE IMAGES FROM FRIENDS YOU TRUST

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

Fear Of Mising Out FOMO



DE-PERSONALISE THE IPHONE / IPAD

New Challenges Continued

Online Challenges

Ice Bucket Challenge

Motivational Challenges
Ice Bucket / Fitness etc

Tik Tok Challenges

Neutral Challenges
Dance / Fruit / Physical etc

Blue Whale Challenge

Parvel Durov

Red Dolphin

Telegram

Com Networks

UK warns of emerging threat from 'sadistic' online 'Com networks' of teenage boys

Discord

- *English-speaking cyber criminals predominantly teenage boys who share sadistic and misogynistic material and have been seen to target those their own age or younger*
- girls as young as 11 "have been coerced into seriously harming or sexually abusing themselves, siblings or pets.
- These groups are not lurking on the dark web, they exist in the same online world and platforms young people use. Young girls who are often groomed into hurting themselves and in some cases, even encouraged to attempt suicide
- Discord was concerned about a group calling itself CVLT
- Girls were forced to join group calls, where they would be instructed to carry out sexual acts and acts of self-harm for their audience. In severe cases, vulnerable victims were encouraged to kill themselves on camera,"

Online Image Financial Extortion (How)

Scams – Viruses - Extortion
Involves being forced *doing things* after an offender has threatened to release inappropriate photos.

This could be a real photo taken by the victim, or a fake image created of them by the offender using Artificial Intelligence (Ai)

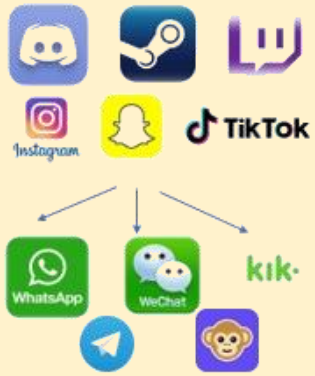
THIS TYPE OF CRIME doubled in 2023, rising to 26,718 compared to 10,731 the year before.

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 motivated by making money quickly, rather than Personal Attack
Blackmailing their victim in under an hour.
CATFISHING

Blackmailed after sharing an image or video, or the offender sharing hacked or digitally Manipulated / AI-generated images with the threat of sharing them wider
Ai Deep Fake Images



SO, REMEMBER

1. Don't get a Virus by opening an unexpected message
2. If You Can make online purchases 'Ask Permission 1st'
3. If You Can – Only Engage with True Friends in Online Games
4. If anyone tries to Trick you always STOP & TELL
5. Parents must check bank statements

Deep Fake

In the 1st technique, it is possible to replace the face of a person shown on an inappropriate image with that of another person, with the aim of creating a deepnude. This technique is called Face Swap

The 2nd technique is the Undress technology. This technology uses artificial intelligence to predict how a depicted person would look 'with no clothes on' based on just one photo. In this case, no additional image is therefore used for the manipulation, but the image of the person is the source material on which the artificial intelligence is programmed.

The 3rd technique no longer starts from a specific image as the source material to create a new naked image, but gathers information from a huge quantity of images to create a completely virtual naked person.

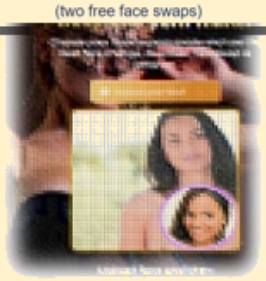
Artificial Intelligence, is making it increasingly easier to create images that appear lifelike.
'DEEP FAKE'

Undress Artificial Intelligence describes a type of tool that uses artificial intelligence to remove clothes of individuals in images.

This Artificial Intelligence technology is therefore not aimed at undressing a real person, but rather at creating a naked image or video of a non-existent person

Try DeepSwap now

(two free face swaps)



The use of deepfake to create a sexual image was first done on the social platform Reddit

The technology is increasingly being used for cybercrime or grooming young people

Deep Fakes

98% of deepfakes are inappropriate in nature

Home Security Heroes (2023)

99% of these deepfakes are of women

The vast majority of Deep Fake apps, (freely available through search engines), focus solely on creating Inappropriate Images of women

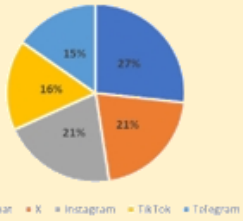
The phenomenon of Deep Nudes can be seen as a reflection of disrespect and objectification

The mental impact of Deep Fake Images are serious and include post-traumatic stress disorder, anxiety disorders, depression, loss of self-confidence and even suicidal thoughts

Whether creating Deep Images is a criminal act- depends on the image created, whether or not there is consent, and the technology used.

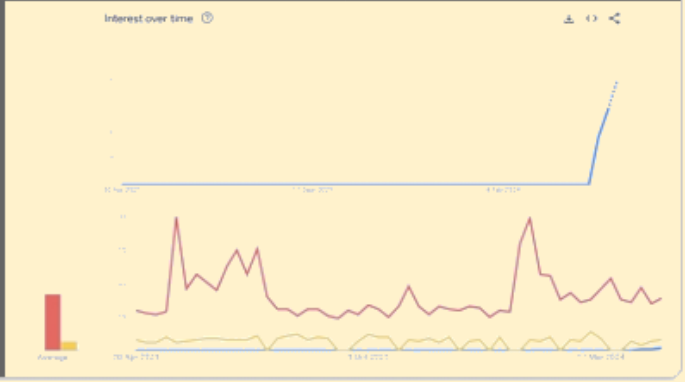
Deep Fake Image ?

Through which platform did you see a deepnude?



Creating a Inappropriate explicit image of a Child (Under 18) is always a criminal act

It does not matter whether the image was of a real child, a manipulated image of a real child, or a virtual image of a non-existent child.



Quick Survey

https://forms.office.com/Pages/DesignPageV2.aspx

New Ideas

Ban Social Media for Un 16's

Ban Smart Phones in Schools

New Plans

TikTok, Instagram, Facebook, Snapchat, X, Reddit, YouTube, Twitch, Threads and Kick

Fake Age Verification
Use of VPNs or Location Masks
Alternative Platforms
Less-Regulated New Services
It will not fully stop under-16 access
It may push children into less safe spaces
Vulnerable children may be most affected

The Challenges of a Blanket Smartphone Ban

Schools must consider:

- Students with medical needs who rely on smartphone apps
- Students with safeguarding or care-related needs
- SEND students who use devices as support tools
- Post-16 students, where independence and preparation for adult life are key expectations
- Alternative devices, such as tablets, smartwatches, or wearable technology
- Travel considerations, including school buses and journeys to and from school

23

"Social Media & Respectful Online Behaviour

There is Hope
What Can You / We Do?

- Think before you take a pic or/ post: Is it kind? Is it respectful? Is it necessary?
- Ask Permission
- Online helplines or child safety organisations
- Speak up if you see abuse
- ?
- Support classmates who are being targeted
- School counsellors and trusted staff
- Report harmful behaviour to a trusted adult
- Reporting tools on social platforms

Don't Have Fears

Fear of being thought of as a snitch

Fear of getting into trouble

Don't Blame Yourself

- Instagram, Snapchat, TikTok— can all be double-edged swords. **(Don't Just 'Like')**
- Most use them for identity, validation, and community—but they also ***fuel***: **(Discuss With Adults)**
- Constant comparison (**You Are Good As You Are**)
- Cyberbullying **(SUPPORT EACH OTHER)**
- Fear of missing out (FOMO)
- Addiction to "likes" and digital approval

Don't Panic About Getting Parents Involved with Your Online Life

Online Safety Guidance New Concepts New Issues

What to 'Take Away'

School Internet Access is Safe
When Students are Asleep, they are Safe
If Children & Young Adults have Unsupervised Access 'AT HOME' They may be 'Unsafe' SO

New Concepts will continue to Evolve

Virtual Reality has an important part to play in Education

Artificial Intelligence has an even more important part to play in Education

Nearly 'ALL' Online Dangers occur as a result of Social Internet Usage

Cyber Flashing is 'Real' – Offenders Cannot be ID'd but be can help possible Victims

Girls remain possible Victims of Sextortion 'but' Boys are now target by Catfishing & AI

Legislation May help but Education is SO Important

AWARENESS KNOWLEDGE ADVICE INVOLVEMENT

Screen Time
Online Challenges
Best Practice
AI & VR
Prejudicial Behaviour
Self Perpetual Radicalisation

Jonathan Taylor *MSc*

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