St. Thomas's Centre

# ONLINE SAFETY UPDATE

SPRING TERM 2024

## SAFER INTERNET DAY

Tuesday 6th February 2024 was Safer Internet Day. We discussed how Artificial Intelligence (AI) is changing our digital world and how to remain aware and safe from deep fakes, photographic and voice cloning.

**Artificial Intelligence (AI)** refers to computer systems that can perform tasks that previously only a human could do. A computer-controlled robot can think similarly to that of a human.

### Deep Fakes

AI is being used to create fake photographs and videos. Celebrities were the first to be targeted but now AI is being used as the latest form of online bullying and fake news amongst our children.

It has been nationally reported that pupils are using AI technology to abuse each other, they are creating indecent images, which legally constitutes to child sexual abuse material. This can have many harmful effects that could lead to blackmail and further abuse.

Imagery of child sexual abuse is illegal in the UK, whether AI generated or photographic – with even cartoon or less realistic depictions still being illegal to make, possess, and distribute.

https://saferinternet.org.uk/blog/children-must-understand-risk-as-uk-schools-say-pupils-abusing-ai-to-make-sexual-imagery-of-other-children

### Voice Cloning

AI is being used for voice cloning. There is already evidence of celebrities and politicians having their voices cloned and used to spread fake news over social media. If criminals can find enough content of you to copy your voice, then you could be open to being a victim of voice cloning. A criminal intentionally clones the voice of a member of your family to blackmail, abuse or scam you. To prevent voice cloning limit who has access to your social media and set up a family password.

https://www.independent.co.uk/tech/ai-voice-clone-scam-kidnapping-b2319083.html

## New Criminal Offences

### Cyber-flashing

This is when someone intentionally sends an unsolicited sexual image or video to someone else via social media, dating apps, or a data sharing service such as Airdrop. It's classed as an offence if the person who sends the image or video intends the recipient to be alarmed, distressed or humiliated, or it is sent for their own sexual gratification.

### Creating or sharing "deepfake" pornography of someone without permission:

This is a pornographic video or photo that's been created using artificial intelligence (AI).
Sending a false communication: a person commits a false communications offence if they:

- Send a message with information that the person knows to be false
- Intend to cause psychological or physical harm
- Have no reasonable excuse for sending the message

### Sending a death threat or threat of serious harm online:

a person commits a threatening communications offence if they:

- Convey a threat of death or serious harm
- Mean for the recipient to fear that the threat would be carried out, or didn't consider whether the recipient would fear this

### Assisting or encouraging someone else online to self-harm:

someone commits this offence if they do something with the intent to encourage or assist someone to seriously self-harm. This is regardless of whether the other person actually self-harms or not.

### Sending a flashing image to try and trigger a seizure in someone with epilepsy:

this is sometimes known as "epilepsy trolling" and was introduced by Zach's Law.

## Online Safety Act 2023 Explained

The Online Safety Act became law in October 2023. Its goal is to make the internet safer for everyone (particularly children) by placing more responsibility on social media platforms and other online companies to protect their users.

Although the Act has been passed, most of it is not yet in force. Ofcom (the UK communications regulator) and the secretary of state need to write the guidance and secondary legislation that will underpin the Act.

It applies to online services, such as:

- Services that host user-generated content (e.g. social media sites such as Facebook and Instagram)
- Search engines (e.g. Google and Bing)
- Services that host pornographic content
- Messaging platforms (e.g. WhatsApp)
- Video-sharing platforms (established in the UK)

**What does it cover?**
Once Ofcom consults on and writes its guidance, the affected services will have to:

- Remove illegal content quickly or prevent it from appearing in the first place
- Prevent children from accessing harmful and age-inappropriate content (for example, pornographic content, content that promotes, encourages or provides instructions for suicide, self-harm or eating disorders, content depicting or encouraging serious violence or bullying content)
- Enforce age limits and use age-checking measures
- Be more transparent about the potential risks and dangers associated with the platforms
- Give parents/carers and children clear and accessible ways to report any problems they have
- There will be sanctions for services that don't follow the Act.

St. Thomas's Centre

# ONLINE SAFETY UPDATE

SPRING TERM 2024

## Steps you can take to help keep your younger children safer online

**Parental controls:** Parental controls have been designed to help you manage your child's online activities. There are various types, some of which are free but others which can be bought. However, nothing is totally fool proof so this shouldn't replace the support and guidance you give your child to help keep them safer. For more information and step by step instructions on setting up parental controls, visit Parental Controls & Privacy Settings Guides - Internet Matters.

**Supervise their online activity:** Keep the devices your child uses in communal areas of the house such as the living room or kitchen, where an adult is able to supervise. Primary-age children should not access the internet in private spaces alone, such as in a bedroom or bathroom.

**Explore together and chat little and often:** Ask your child to show you their favourite apps, games and sites and encourage them to teach you how to use these. Ask them if anything ever worries them online. Make sure they know they won't be in trouble and can get help by talking to you or another adult they trust if anything happens online that makes them feel worried, sad or scared.

## Steps you can take to help keep your teenagers safer online

**Have an ongoing conversation**: Continue to talk about the apps, games and sites they like to use, and what they like and don't like and any concerns about being online. Discuss with them when to unfollow, block or report. For help starting this conversation, read having a conversation with your child.

**Make sure they know where to go for support:** Remind your child they can always speak to you or an adult they trust if anything happens online that makes them feel worried or upset. Remind them that they won't be in trouble at that you are there to help. For a breakdown of report services, visit:
Supporting your child with reporting unwanted content online

**Make sure they know about NCA CEOP:** Young people can report a concern about grooming or sexual abuse to NCA CEOP at https://www.ceop.police.uk/safety-centre/ and get support from a specialist Child Protection Advisor.

## More information?

**Thinkuknow is the education programme from the National Crime Agency's Child Protection Command CEOP (NCA-CEOP) whose aim is to protect children and young people from sexual abuse online.**

**For more information, advice and guidance, visit their parent's website and download their home activity worksheets for fun, online safety activities to do with your family.**

**https://www.thinkuknow.co.uk/parents/**