SPOTLIGHT ON SAFEGUARDING

Working together to keep our young people safe

In this month's issue:
- Sextortion
- Gaming
- App focus: Playstation and Xbox

Primary | May 2024

Sextortion – what is it?

Sextortion is a type of blackmail in which the offender threatens to disclose sexual content, such as information, photos or videos of the victim, with the intention of extorting money from them. Another phrase used to describe sextortion is *'online sexual coercion and extortion'*

How are children sextorted?

Individuals pretending to be children of the same age as the victim build a relationship with the young person over hours, days or even weeks. Once trust is established, the perpetrator begins to ask the young person for intimate images and videos. The victim sends the requested content, unaware that they are communicating with a criminal.
Self-generated Child Sexual Abuse Material (CSAM) refers to instances where a child produces images or videos of themselves, or agrees to someone else creating such content, such as through video calls. It's crucial to understand that in these situations, the child is coerced, manipulated or pressured into participating, making them a victim.
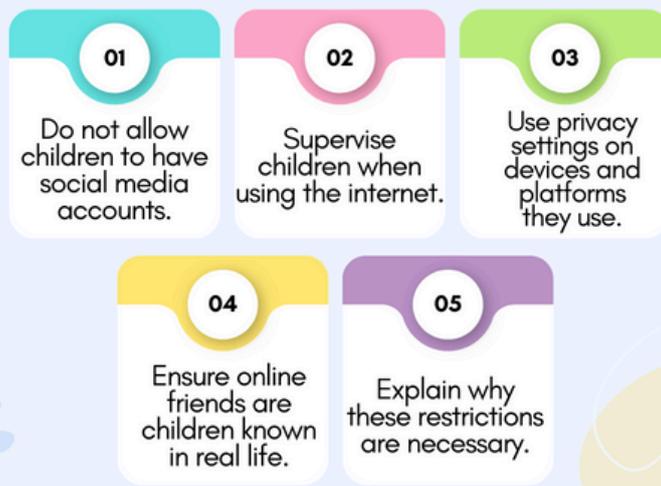
What are deepfakes?

With the capability to generate highly advanced AI images, children face increased vulnerability as criminals exploit fake images to extort them.
Deepfakes refer to AI-generated images where one person's face is substituted with another. These creations can be incredibly realistic, making it challenging to distinguish between what is genuine and what is fabricated.
The worrying part about AI-generated images is that the victim might never have shared any images with the perpetrator. However, due to fear and persuasion, they may agree to pay money to prevent the release of these fabricated images to friends and family.

5 Ways to Protect your Child from Sextortion

01 Do not allow children to have social media accounts.

02 Supervise children when using the internet.

03 Use privacy settings on devices and platforms they use.

04 Ensure online friends are children known in real life.

05 Explain why these restrictions are necessary.

Steps to take if your child is a victim of sextortion

1 GIVE THEM YOUR SUPPORT
They might be experiencing distress. Reassure them that they are a victim and that you are here to support them.

2 DON'T PAY ANY MONEY
Avoid interacting with the offenders or giving them any money. Block them on all platforms where your child may have interacted with them.

3 COLLECT EVIDENCE
Capture screenshots of conversations, images and any interactions your child has had with the perpetrator as evidence.

4 REPORT TO THE POLICE
This can be done through your local Police service online. It is crucial for the Police to prevent the perpetrator from targeting anyone else.

5 REPORT ON THE PLATFORM
Report the incident on the platform where it occurred. This action will assist the platform in safeguarding other users from such perpetrators.

6 SPEAK TO SCHOOL
School staff are available to support your child and handle any situations that may arise in school if any images are leaked.

SPOTLIGHT ON SAFEGUARDING

Gaming

Gaming encompasses playing games on various devices such as Xbox, smartphones, laptops, or computers. It is often a social activity where friends compete or play together. However, negative behaviours and consequences can arise from gaming. Some concerns include:

- excessive gaming leading to addiction
- playing games with inappropriate content
- sharing personal information
- interacting with unknown individuals, including adults posing risks
- cyberbullying
- in-app purchases leading to gambling
- displaying verbal or physical aggression
- poor eating habits
- sleep disturbances

These issues can impact children's mental health and relationships. It is crucial to monitor gaming to prevent excessive use, safeguard children's accounts and devices, and ensure games are suitable for their age and development.

How to keep your child safe whilst gaming

01 Get to know the games they play to understand why they enjoy them.

02 Enable 'airplane' mode for young children's devices to prevent online interactions.

03 Refer to the PEGI ratings as a reference to determine if the content is age appropriate.

04 Teach them how they can block and report other users, should they need to.

05 Monitor who they are connecting with whilst they are playing.

06 Establish boundaries like setting daily time limits and screen-free activities.

07 Teach them how to behave positively whilst gaming.

PlayStation Network App

The PlayStation app enables users to remain connected even when they're not actively gaming. Users can share photos, videos and other content, as well as engage with online gaming communities. However, there is a potential risk of interacting with unfamiliar adults and encountering inappropriate content. Each child account includes parental control features. For detailed instructions on using these settings, visit the PlayStation website. Click here

Xbox App

The Xbox app allows users to connect with one another, continue gaming and join 'Parties'. Parties are when groups of players play alongside one another. There are risks associated with them, as anyone can join, leaving young people vulnerable to having contact with unknown adults.

All child accounts have safety features which allows parents to implement privacy settings as well as set time limits. Click Here

Click for The Enlightened Parent