Cotham School
Online Safety Newsletter

Academic Year: 2025/2026

Term: 3
Date: 26/01/2026

Newsletter Topic:

1. What is: A Deepfake
2. Social Media Focus: Instagram - Public and Private Accounts

Deepfake?

A 'deepfake' generates photos, videos and audio via AI models trained on the subject to mimic their look and sound, making it appear they said words or committed acts that never occurred.

Why This Matters

With a recent report from The Alan Turing Institute finding that over 90% of people in the UK have encountered misinformation online, it's more important than ever to equip our children—and ourselves—with the tools to navigate the digital world safely. This includes understanding new threats like deepfakes.

Risks of deepfakes

- **Fake News:** Deepfakes are increasingly used to spread fake news, propaganda, and scams, as the technology becomes easier to use and public figures provide ample material for AI training. For example, in 2023, propagandists on X circulated an audio deepfake of Labour leader Sir Keir Starmer that falsely portrayed him berating an aide.
- **Scams:** Scammers use deepfakes of anyone's voice or likeness to commit fraud. In 2019, criminals impersonated a CEO's voice to steal €220,000, and in 2023, an Arizona mother received a fake kidnapping call featuring a deepfake of her daughter's voice.
- **Extortion:** Deepfakes can also make you a target of blackmail, even if you've done nothing wrong. Criminals can fabricate compromising videos using your likeness to extort money, despite the scenes being completely fake.
- **Explicit Material:** The vast majority of deepfakes (96% in a 2019 report) are non-consensual pornographic videos, created by superimposing a person's face onto an actor's body. This harmful practice is not only a violation in itself but also a common tool for extortion, a threat highlighted by the FBI in 2023.

Advice for Parents & Educators

Keep profiles private

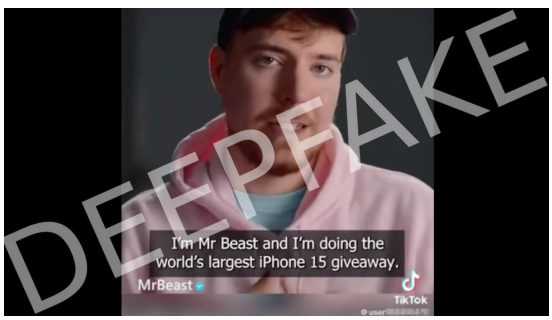
Crafting a believable deepfake requires access to a person's photos, voice clips, or videos. Since everyday individuals often share such content publicly on social media, these platforms become prime sources for gathering material. To reduce this risk, use the privacy controls offered by social media sites to restrict who can view and download your personal content.

Looks for Signs

Although deepfake technology has advanced significantly, there are still detectable clues. Visually, look for blurriness, flickering, or unnatural textures around features like hair and teeth. The mouth may also move out of sync with the spoken words. In audio deepfakes, listen for mispronunciations and a flat, robotic speech pattern.

Research and inform your children

Research suspicious content and inform your children. For advanced deepfakes with no clear flaws, use critical thinking and verification: contact people you know directly about questionable videos and check reliable sources for public figures—always consider the creator's motive, look to trusted news sources. Always ask: 'Who made this, and why?'. Simultaneously, educate children on why deepfakes are harmful. As the technology becomes more accessible, young people may misuse it. Teach them the ethics and real-world damage of manipulating someone's image without consent.



How to spot an AI Generated Video: https://www.bbc.co.uk/news/videos/c050eq4llpro

With deepfake tools becoming more accessible and misinformation affecting almost everyone online, we must explain that manipulating someone's image isn't just a trick—it can cause real harm and is a serious form of misuse.

Source: The National College, The Turing Institute.

Cotham School
Online Safety Newsletter

Academic Year: 2025/2026

Term: 3
Date: 26/01/2026

Social Media: Instagram
Instagram is a social media platform focused on sharing photos, videos, and stories. It allows users to connect with friends, follow their favorite creators, and discover content through a visually driven feed. Instagram is owned by Meta (formerly Facebook) and is widely used for personal sharing, influencer marketing, and business promotion.

Age Requirements: 13+.

Key Features:
- Feeds
- Stories
- Reels
- Live streaming
- Explore page
- Direct messaging
- Filters and image editing

Safety and Privacy Features:
- Private accounts
- Comment controls
- Restricting negative accounts - bullying
- Parent supervision - link parent to teen accounts
- Report and block
- Age restrictions
- 2FA security
- Activity dashboard

How to: Manage Privacy Settings
If under 18, Instagram accounts are private by default. Users under 16 need parental permission to go public, while 16–17-year-olds can change it unless they have parental supervision enabled.

Make your account private
- Click More icon, ☰, then click ⚙ Settings.
- Click Account privacy below Who can see your content.
- Click ⬭ Toggle next to Private account to make your account private.
- Click Switch to private to confirm.
- Bear in mind that business profiles aren't able to make their accounts private.

The differences between public and private accounts on Instagram:

	Public	Private
Who can follow you?	Anyone on Instagram	Only people you approve
Who can see public accounts that you follow and that follow you?	Anyone on Instagram	Anyone on Instagram
Who can see private accounts that you follow and private accounts that follow you? Who can see your photos and videos on your profile or in feed?	Anyone on Instagram	Your followers
Who can see your profile information, including your profile photo, name, username and bio?	Anyone on or off Instagram	Anyone on or off Instagram
Who can share your photos and videos with other people on Instagram and see what's shared?	Anyone on Instagram, unless you update your settings	Your followers, unless you update your settings
Who can remix your videos and download your reel?	Anyone on Instagram, unless you update your settings	No one
Who can embed your photos and videos off Instagram? Who can see links to your photos and videos in search engine results?	Anyone on or off Instagram	No one