Ashley Junior School

Mr Cousins ICT Systems Manager

Online Safety Newsletter January 2026

Instagram Teen Accounts - update

You must be over 13 years of age to set up an account. Instagram is used to post photos and videos as well as send direct messages, make voice/video calls, and send disappearing messages.

Teen accounts are automatically set up for users aged 13 – 17. Instagram have announced that teens will now see content similar to content that they would see in a PG-13 movie.

Instagram have also updated their policies around content to include "hiding or not recommending posts with strong language, certain risky stunts, and additional content that could encourage potentially harmful behaviors"

Finally, for parents who would like to apply more stringent settings, Instagram are also introducing a new, stricter setting called 'Limited Content.' This setting will mean your child is not able to see, leave, or receive comments under posts as well.

You can read about the updates here: https://about.instagram.com/blog/announcements/instagram-teen-content-safety-pg-13

Roblox

Following a recent ITV investigation*, which found extremist content on Roblox, we thought we would provide a reminder of what you need to be aware of.

Roblox is a platform consisting of a collection of games. Players can either create games or play games that other users have created. It is free to download (however subscription options and in game/app purchases are available) and can be played across numerous devices. **A lot of the content is user generated, which means not all games will be suitable for your child to view/play.** If your child is playing Roblox, it is important to monitor what your child is accessing and set up appropriate parental controls. **PEGI rate Roblox with a Parental Guidance label, this is because it is considered a platform with a huge level of user generated content.**

What should I be aware of?

Game content – as mentioned, users create games so the content/themes may not be appropriate for your child. Roblox label content based on the type of content rather than by age. The labels are Minimal, Mild, Moderate and Restricted.
Chat Facility - Players can chat with each other (users under the age of 13 need parent permission to access certain chat features though). You can turn communication off completely or add restrictions, such as only able to communicate with friends.
Virtual Currency - Players can buy Robux (their virtual currency) to buy in-game upgrades or accessories.

How do I report abuse and block users?

This article outlines the different reporting facilities:
https://en.help.roblox.com/hc/en-us/articles/203312410-How-to-Report-Rule-Violations

What else can I do?

Chat to your child regularly about what they are doing online and remind your child that if anything is worrying them, then they should talk to you or another trusted adult.

Further information

https://parentzone.org.uk/article/roblox

[*Source: https://www.itv.com/news/2025-11-14/mosque-attacks-and-far-right-skins-roblox-teens-exposed-to-extremist-content]

Family Smart Start

Family Smart Start is a free toolkit designed to help you and your child navigate the milestone of getting their first phone. The toolkit
provides support on how to set up their new phone, how to talk to your child about digital safety and a template family agreement. Find out more here:

https://familysmartstart.com/

What Parents & Educators Need to Know about

AI-ENABLED SCAMS

WHAT ARE THE RISKS?

Artificial intelligence (AI) is quickly becoming a widely used tool, with lots of positive applications being discussed and developed. Sadly, however, as with most technology tools, there are those who will seek to use it for malicious and dishonest practices, with children and other vulnerable groups particularly at risk.

PHISHING EMAILS: BETTER & QUICKER

Phishing scams – emails designed to trick people into handing over login details or money – are not new, and do not rely on AI; however, AI has made them far more dangerous. Criminals can now generate highly convincing emails at speed, mimicking an organisation's tone, branding and language with ease. This makes phishing attempts harder to spot, especially for young people who may not yet know what to look out for.

ONLINE MARKETPLACE FRAUD

Online marketplaces are now a common way to buy and sell everything, from second-hand clothes to cars. Criminals are exploiting this by using AI to enhance or completely fake product photos and videos, and pressure buyers into paying deposits or full amounts upfront. These tactics are becoming more advanced, making it vital to pause, check, and verify the sale before parting with any money.

VOICE IMPERSONATION

AI can now realistically impersonate a person's voice when given a small sample of someone's speech patterns. This is especially concerning where voice has been enabled as an alternative to password-based logins. One such example was the use of AI deepfake audio as part of a fake kidnapping scam: the criminals used an AI voice clone of a 15-year-old to convince her parents she had been kidnapped and elicit a ransom.

EMPLOYMENT SCAMS

Using AI, criminals can create fake online profiles that seem completely real. These synthetic identities can chat with young people about fake job offers, asking for money to secure a visa or paperwork. In 2025, The Guardian reported a scam targeting young people with promises of quick cash, posing as TikTok staff.

INFLUENCER & INVESTMENT SCAMS

AI tools now make it easy to manipulate video and audio, with technology available that can generate entirely fake content using the likeness of celebrities or influencers. Criminals are using this to create convincing videos of well-known figures promoting fake products or services, which young people can be particularly susceptible to. Cryptocurrency scams are a common tactic, luring people into investing in schemes that do not exist. Once payment is made, the criminal simply disappears with the money.

ROMANCE SCAMS & SEXTORTION

AI chat bots can now mimic real conversations, often accompanied with realistic fake photos and videos, which makes it easier for criminals to build trust with young people – among other things, this can lead to fraud or sextortion. In 2024, the NCA's CEOP Safety Centre received 380 reports of sextortion. Alarmingly, in the first five months alone, police received an average of 117 monthly reports involving under-18s, showing how serious and targeted this threat has become.

Advice for Parents & Educators

THINK CRITICALLY

The key to addressing the increasing growth of AI-enabled scams is to think critically and show caution. Inform children that if something is too good to be true, then it probably is. Encourage them to stop and carefully consider what they are seeing and reading before taking any action. For example, if a social media post expresses urgency, proceed with caution; if content seems unusual, even from a known person, it may be that their account has been hacked.

USE TRUSTWORTHY SITES AND SERVICES

Online marketplaces are useful when buying and selling items; however, where possible, encourage children to use reputable companies and their online shopping sites. These companies are likely to have more sophisticated cyber-security safeguards in place, underpinned by consumer legislation, enabling them to control how products and services are displayed and traded on their sites.

SEEK TO VERIFY

Criminals may breach an influencer's account or spread misinformation and fake content; however, their approach will generally be limited to a single account, site or service. Where possible, show children how to verify information to check its legitimacy before proceeding. Small actions, such as phoning the person who is the subject of a suspicious email, or checking content via an individual or company website or social media sites can make the difference. The greater the risk, the more effort we should expend to confirm whether the information presented is true or false.

REPORT IT

As the sophistication of scams increases, the likelihood of being tricked by them also increases, especially when not paying attention or acting quickly. It is important that young people know how to report incidents as they happen. Show children how to report their concerns to the social media site, Action Fraud, banks, and other individuals or organisations linked or involved. If you are unsure of the most effective reporting channel, contact Action Fraud.

Meet Our Expert

Gary Henderson is the Director of IT at Millfield, a large independent boarding school in Somerset, as well as a member of the Digital Futures Group, Vice Chair of the ISC Digital Advisory Group and an Association of Network Managers in Education (ANME) Ambassador.

#WakeUpWednesday®

The National College®