Ashley Junior School

Mr Cousins ICT Systems Manager

Online Safety Newsletter February 2026

CBeebies Parenting and Apps

CBeebies Parenting is full of useful information from creative activities, recipes and information about the CBeebies apps.

CBeebies apps are free to download with no in-app purchases. Their apps include:

- Playtime Island - Fun Games for Kids App. This app includes 40 free games.
- CBeebies Learn - Early Years Learning App. This app includes games and videos and is based on the Early Years Foundation Stage curriculum.
- Get Creative - Open-ended Creative Activities App. This app is free and includes lots of drawing and painting activities.
- Storytime - Reading Stories App. This app includes interactive story books.

You can find out more here:

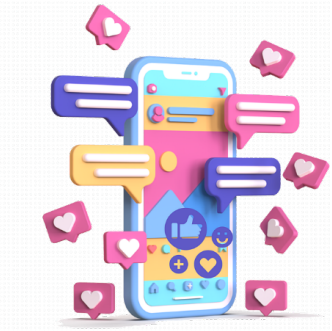
https://www.bbc.co.uk/cbeebies/parenting

Balance screen time tips

Internet Matters have created simple tips to help you develop healthy online habits for your child. They also answer key questions such as "how much screentime is too much" and "is gaming bad for children." Access this information here:

Screen Time Link

TikTok



You must be over 13 years of age to use TikTok. TikTok is a social media platform for sharing and watching short video clips. If your child is using TikTok then make sure appropriate security / privacy settings are applied.

Account set up

It is important that your child enters their real date of birth as accounts are tailored by age e.g., Direct Messaging is disabled for accounts aged 13-15. In addition, advertisements are tailored by age. By default, accounts for people under 16 are set to private. You can read more about the other settings available, such as switching off comments and restricted mode here: https://support.tiktok.com/en/account-and-privacy/account-privacysettings/privacy-and-safety-settings-for-users-under-age-18

Family Pairing

Family Pairing allows you to link your own account to your child's account. You can then set controls such as restricted mode or tailor your child's 'For You' feed by selecting keywords that TikTok will use to filter out posts. You can find out more here: https://support.tiktok.com/en/safety-hc/accountand-user-safety/family-pairing

What do I need to be aware of?

- Inappropriate content and themes: whilst against guidelines explicitandin appropriate content can be found on this platform, for example nudity/sexual content and hate speech. Some of the songs available to lip sync to may contain inappropriate lyrics/themes.
- Challenges: We often see viral challenges on social media, some of which can be risky/dangerous. Sadly, there are reports that children have died whilst attempting online challenges. Children may not yet have developed the skills and ability to critically analyse that what they see online is not always safe for them to replicate.
- Stranger contact: chat to your child about how people may not be who they say they are when online.

Refresh your feed

You can refresh your "For You" feed to update the content recommended: https://support.tiktok.com/en/account-and-privacy/account-privacysettings/refresh-your-for-you-feed

Blocking and Reporting

Show your child how to use the safety features available.

Further information

- https://parentzone.org.uk/article/tiktok
- https://www.tiktok.com/safety/en/guardians-guide

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®