At The National College, our WakeUpWednesday guides empower and equip parents, carers and educators with the confidence and practical skills to be able to have informed and age-appropriate conversations with children about online safety, mental health and wellbeing, and climate change. Formerly delivered by National Online Safety, these guides now address wider topics and themes. For further guides, hints and tips, please visit nationalcollege.com.

What Parents & Educators Need to Know about VPNs

VPN use among UK teens is on the rise – with a noticeable uptick following the introduction of the Online Safety Act's age-verification rules. A VPN – or virtual private network – can boost online privacy by hiding internet activity and masking the user's location. But while this technology has legitimate uses, it can also allow children to bypass safety filters and access inappropriate content. This guide covers what parents and educators need to know about VPNs and how to keep young people safe.

WHAT ARE THE RISKS?

BYPASSING RESTRICTIONS

VPNs are commonly used by young people to get around blocks on school networks or parental controls. This could include accessing social media, gaming sites or adult content that would otherwise be filtered out.

ACCESSING INAPPROPRIATE CONTENT

When a VPN is active, content filters can no longer see which sites a child is visiting. This means they could access inappropriate content without detection. This also makes it harder to intervene when a child is engaging in risky behaviour, as it may be difficult to detect it's happening.

REDUCED TRANSPARENCY

VPNs may make parental monitoring software ineffective, stopping parents from monitoring their child's activities, including their ability to identify potentially harmful or inappropriate content or online contact. This in turn may prevent parents from protecting their children from attempted sextortion or other online threats.

FALSE SENSE OF ANONYMITY

Children believing that VPNs make them 'invisible' online may seek to explore unsuitable internet content, including content which might otherwise be blocked. This may result in them seeking and accessing increasingly inappropriate – or even harmful – content.

INCREASED EXPOSURE TO MALWARE

Many free VPN apps are poorly regulated and may carry hidden malware. Young people installing unverified software could unknowingly open up their device (and home network) to spying, data theft, computer viruses, or even remote access by criminals.

RISK OF MALICIOUS VPN PROVIDERS

Although VPNs may increase privacy from network or service provider filtering and monitoring, this results in providing user and usage data to VPN providers. Some VPN providers may track user activity and sell that data to advertisers – or worse, malicious third parties. Not all VPNs are trustworthy.

Advice for Parents & Educators

EXPLAIN THE POSSIBLE BENEFITS OF VPNS

Explain how VPNs can help protect user data and therefore may be appropriate when using public or other unsecured Wi-Fi, or while dealing with sensitive corporate or personal data.

EXPLAIN THE RISKS OF VPNS

Discuss online risks, including harmful, disturbing, and criminal content. Inform children about criminal contact, such as sextortion, and how VPNs may restrict adults from monitoring children's internet use and helping them avoid these risks.

FREE ISN'T FREE

Discuss the risk of 'free' VPNs and how they may sell or use people's data, which adds privacy risks. Additionally, discuss the potential for added malware in VPN downloads, and how these compromise devices and apps, leading to potential fraud or theft.

CHECK DEVICES FOR VPNS

VPNs can be installed as both apps and browser extensions, so regularly check these on the devices used by the young people in your care. If they have been using VPNs, discuss it, listen to their reasoning, and inform them of the associated risks. In some cases, it may be appropriate to block VPN use via parental controls and other settings.

DISCUSS ONLINE BOUNDARIES

Reinforce the importance of keeping safe online and how filtering and monitoring helps keep young people safe – explain this to them rather than just 'being strict'. Encourage an open conversation around what they're accessing and why.

Meet Our Expert

This guide has been created in collaboration with Gary Henderson, director of IT at a large independent school in the UK, an ambassador for the Association of Network Managers in Education and the Vice Chair of the Independent Schools Council Digital Advisory Group.

#WakeUpWednesday®

The National College®

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 20.08.2025