digitalsafety
DIGITAL SAFETY FOR ALL

Winter 2026

ONLINE SAFETY NEWSLETTER





> *"Welcome to the fourteenth edition of Digital Safety's half termly bulletin. This edition contains information of what is currently happening in the online world."*
>
> **Stuart Younger Cooper, Digital Safety CIC**



Welcome to the winter edition of the Digital Safety Online Safety Newsletter.

As we approach the end of another busy year, the online world continues to evolve, bringing new opportunities alongside challenges for schools, parents and young people.

With the festive break approaching, it's a particularly important time to stay informed about the platforms, technologies and online behaviours that can affect children's safety and wellbeing.

In this edition, we're exploring some of the latest developments and sharing practical advice to help schools and families navigate them with confidence.

This edition includes:

- Snapchat's new 'Now Playing' feature – what parents need to know about music sharing, location settings and children's online privacy.
- Children using VPNs – why young people are using Virtual Private Networks, the potential risks and how parents can start informed conversations.
- Cyber Essentials and school security - why checking suppliers' cyber security matters, alongside information about new funding for eligible businesses.
- Supporting safer digital communities - how Digital Safety CIC can help schools strengthen online safeguarding, cyber resilience and staff awareness.

Our aim remains simple: to provide clear, relevant information that helps schools and families better understand today's digital environment and take practical steps to stay safer online.

As the year draws to a close, we'd also like to thank the schools, partners and communities we've worked with throughout 2026.

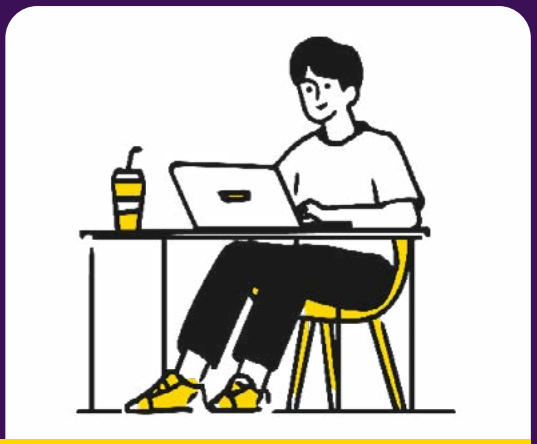
From everyone at Digital Safety CIC, we wish you a happy, healthy and safe festive season.

Stuart Younger Cooper
Digital Safety CIC

digitalsafety

DIGITAL SAFETY FOR ALL

ONLINE SAFETY NEWSLETTER



Staff Edition

Snapchat's New "Now Playing" Feature - What Parents Need to Know

If your young person uses Snapchat, there's a new feature rolling out right now that's worth knowing about.

It's called "Now Playing", and it lets Snapchat users share the music they're listening to in real time. On the surface, it sounds harmless enough. But there are a few things every parent should understand about how it works, where it lives inside the app, and what it could reveal about your child, in particular their location.

What exactly is the Snapchat Now Playing feature

Snapchat has teamed up with Spotify (with other streaming services expected to follow) to let users link their music account to Snapchat. Once connected, friends can see what song your child is listening to - live, as it happens.

There's also a music discovery side to it. If your child spots a song they like in a Spotlight video (Snapchat's version of TikTok), they can save it straight to their Spotify account.

Music sharing between friends? Nothing new there. Teens have been swapping songs and playlists forever. Back in my day, it was cassette tapes, then CDs (yes, I'm that old)



The bit parents need to pay attention to

Snapchat Now Playing feature lives inside Snap Map.

If you've been following my content for a while, you'll know Snap Map is the feature I regularly mention to parents. It's the map inside Snapchat that can show your child's real-time location to their friends.

So now, alongside where your child is, Snap Map can also show what they're doing, right down to the song playing in their headphones.

Individually, these are small pieces of information. Together, they paint a much richer, live picture of your child's day. And if their friend list includes people they don't actually know in real life, which is far more common than most parents realise, that picture is visible to strangers too.

digitalsafety

DIGITAL SAFETY FOR ALL

ONLINE SAFETY NEWSLETTER



Staff Edition

Sharing keeps running in the background

Once switched on, listening activity keeps being shared for as long as Snapchat has been opened in the past 24 hours. It only pauses automatically after more than a full day of not opening the app.

Now think about how often the average teen opens Snapchat. Ten times a day? Twenty? In practice, that means sharing is effectively always on, even when they've closed the app and moved on with their day. Your child could be broadcasting their listening activity without even realising.

Real-time listening can reveal more than just music taste: that they are awake late at night, home alone, or in a certain mood. Small signals, but signals all the same. And linking a Spotify account to Snapchat is one more connection between apps, and one more casual "yes" to sharing data across platforms.

The reassuring side;

Now, to be fair to Snapchat, there are some controls built into this feature:

• Your child chooses who can see their listening activity. It's not automatically visible to everyone.

• It doesn't show listening history. Only what's playing right now, no last-played songs, no archive of what they've listened to.

• Sharing can be paused for three hours, 24 hours, or switched off indefinitely.

• It stops automatically if the app hasn't been opened for more than 24 hours.

These are better privacy controls than we've seen on some features in the past. The key, as always, is making sure your child actually knows they exist, and uses them.

What to do this week

Here's my helpful guidance:

1. Sit down with your child and ask if they've seen the feature yet. Lead with curiosity, not concern - "Have you tried this new music thing on Snapchat?" opens a much better conversation than "What are you sharing now?"

2. Check who can see their listening activity if they've switched it on and make sure it's set to actual friends only.

3. Review their Snap Map settings while you're there. Are they in Ghost Mode? Who can see their location? This new feature makes those settings matter even more.

4. Go through their friend list together. The rule stays the same: if they don't know them in real life, they shouldn't be on the list. Check out Snapchat's parental controls

5. Talk about linked accounts. Connecting apps together is so normal now that

digitalsafety

DIGITAL SAFETY FOR ALL

ONLINE SAFETY NEWSLETTER



Staff Edition

most young people never stop to think about it. It's a great habit to build early: pause before you press "connect."

The bigger picture

Features like Now Playing aren't designed to put young people at risk; they're designed to keep them on the app longer and make it feel more social. But every new "live" feature adds another layer to what your child is broadcasting and sharing about their day.

The apps will keep changing. The conversation at home is what stays constant.

Stay informed



Let's work together to raise a generation that uses technology not just for convenience but for building a more informed, compassionate, and connected world.

Stay curious, stay critical, and stay open!

Learn about SNAPCHAT here

Children Using VPNs A Guide for Parents

Children Using VPNs: A Plain-English Guide for Parents by Wayne Denner

Children finding workarounds isn't something new. When I was a teenager, my parents put a little lock on the rotary dial of our phone to stop me running up the bill. It didn't last long. I worked out that if you tapped the receiver hook rapidly (the button the handset rests on), you could mimic the dial's clicks and ring a number anyway.



for more info contact Digital Safety info@ds-cic.com

digitalsafety

DIGITAL SAFETY FOR ALL

ONLINE SAFETY NEWSLETTER



Staff Edition

And if my fingers weren't quick enough, there was always the extension phone upstairs that nobody had thought to lock. Course, back then the worst that happened was a shock on the phone bill and a telling-off

So, it should come as no surprise that finding ways around parental controls is very possible. Today, one of the most talked-about is the VPN.

At a workshop in September, a mum called Sarah put her hand up near the end. Her 14-year-old son had a new app on his phone, and when she asked about it he said, "It's just a VPN, everyone has one." She didn't know what that meant, whether she should be worried, or what to say next. Her question to me was simple: "Is this something I should be worried about?"

You're not alone

If you've had the same thought as Sarah, you're in good company. These are exactly the right questions to be asking, and plenty of parents in my workshops are asking them too.
So what actually is a VPN? It stands for Virtual Private Network. In plain English, it's an app that hides where your internet connection is coming from. It wraps everything you do online in a protective tunnel and makes it look as if you're somewhere else, perhaps another town or even another country.

Think of it like posting a letter inside a second envelope with someone else's return address on it. The post still gets there, but nobody along the way can easily see who sent it or what's inside.

The good news first

VPNs can and do help with privacy and safety. Millions of adults use them every day, often because their employers require it.

They protect privacy. A VPN makes it much harder for anyone snooping on public Wi-Fi in a café or on a train to see what you're doing. That's genuinely useful.

Most use them for ordinary reasons. Ofcom found that 25% of children aged 11 to 17 had used a VPN in the past six months (Ofcom, Children's Use of VPNs, 2026). If we dig a little further into the data, boys use them more than girls (28% vs 20%). About a third of children watching TV, sport or films not available in the UK used a VPN (34%). What is also interesting is that 35% of children took steps to protect their privacy online, with girls more so (40%).

Parents are often already involved. Government research from July found parents are frequently part of the picture, and many children's paid VPNs are bought by mum or dad (DSIT, Children's Circumvention Behaviours Online, 2026). So, it isn't always sneaky.

digitalsafety

DIGITAL SAFETY FOR ALL

ONLINE SAFETY NEWSLETTER



Staff Edition

The risks

Getting round age checks. Since July 2025, UK law has required sites that host adult content to verify users' ages. With a VPN, a user can appear to be in another country, where those checks don't apply. A study found that 7% of all children use a VPN to access age-restricted websites, apps, or games.

Switching parental controls off. Research from Childnet found that 16% of children who use VPNs had used them to get around parental controls. Whatever you lock, someone in Year 9 knows the workaround, even with the phone pouches.

Free VPNs aren't really free. Many free apps make their money by collecting and selling your data, showing adverts, or worse. Some are poorly built and can carry malware (software that can damage your device or steal information). Ironic, for apps sold on privacy.

Landing in the wild west. By appearing to be abroad, children can end up on sites in countries with little or no online safety regulation, where content is far less moderated.

What to look out for:

- A new app with a key, shield or globe icon, or a name with "VPN", "proxy" or "secure" in it
- A small key symbol or the letters "VPN" at the top of their phone screen
- Your parental controls suddenly seem to have stopped working
- Adverts or websites showing up in a foreign language or with foreign prices
- An unexpected subscription on your bank statement or app store account

What you can do

1. **Find out first, don't assume**. Ask your child what the VPN is for. It may be gaming, privacy or watching a match. Their answer tells you a lot.

2. **Check their devices together.** Look through the apps and the smartphone settings (on most phones, search "VPN" in Settings). Doing it side by side feels very different from a secret search.

3. **Block new app installs without your OK.** Apple's Screen Time and Google's Family Link let you approve downloads, so a VPN can't just appear overnight.

4. **Set controls at the router too**. Your broadband provider's parental controls work on every device in the house. Some routers can also block VPN connections. It's worth a quick call to your provider.

5. **Steer clear of free VPNs**. If your family does need one, choose a reputable paid service, set it up yourself and keep the login. I don't recommend letting children pick their own.

for more info contact Digital Safety info@ds-cic.com

digitalsafety

DIGITAL SAFETY FOR ALL

ONLINE SAFETY NEWSLETTER



Staff Edition

6. **Keep an eye on your bank and app store statements**. A surprise subscription is often the first clue. Nobody wants a nasty surprise on a bank statement.

Conversation beats controls

Here's the truth: settings help, but no setting is 100% reliable. If a determined teenager wants to get round something, they usually will. That's why talking matters far more than any app.

Ask open questions like "What do your friends use VPNs for?" rather than "Are you using one to look at things you shouldn't?" One starts a chat. The other ends it.

Most importantly, make sure your child knows they can come to you if they see something upsetting, even if they accessed it via a VPN. If the price of telling you is losing their phone, they'll stop telling you. I recommend the same approach with any tech: deal with the problem first, and the rule-breaking second.

Back to Sarah

So, should Sarah be panicking? No. Her son might be using his VPN for exactly the reasons mentioned in the research above. He might not be. The only way to find out is to ask, calmly and with genuine curiosity.

If it turns out he wants to keep it, that doesn't mean you have to say yes. But it might mean agreeing which VPN, who sets it up, and what it's for.

There's no single right answer for every family. My phone-tapping days ended with a chat round the kitchen table once the bill arrived, and with some time off playing Super Mario Bros.



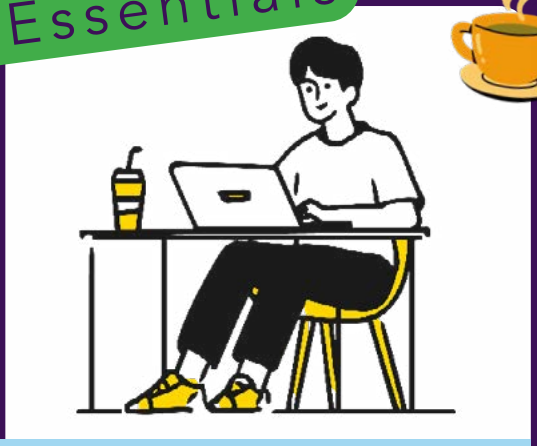
Learn about VPN's here

Learn about the Governement Research here



digitalsafety
DIGITAL SAFETY FOR ALL

75% off Cyber Essentials



December Edition

Cyber Essentials: protecting schools beyond the school gate

Barbara Spooner, MBE, CEO, Digital Safety CIC



Why checking your suppliers' cyber security matters

Schools depend on external providers for learning platforms, payroll and more. A cyberattack on one supplier can disrupt many schools and expose sensitive information. Checking suppliers' security is therefore as important as protecting your own systems.



Two recognised levels of protection

CYBER ESSENTIALS
An independently assessed self-assessment covering five basic technical security controls.

CYBER ESSENTIALS PLUS
The same five controls, with additional independent technical testing.

Why this matters now

The government's 2026 Cyber Resilience Pledge asks major organisations to take a risk-based approach to supplier cyber security. It does not ban uncertified suppliers, but expectations are rising. DfE guidance encourages schools to check whether outsourced IT providers hold Cyber Essentials certification.

New funding: 75% off for eligible SMEs

A new government fund gives eligible UK SMEs 75% off their first Cyber Essentials certification (£80–£125 plus VAT). Applicants must not have held certification in the previous four years. Funding is first come, first served until March 2027 or earlier if exhausted, and remains available through a Certification Body. Schools should check eligibility; it is not a universal school discount.

Digital Safety can help

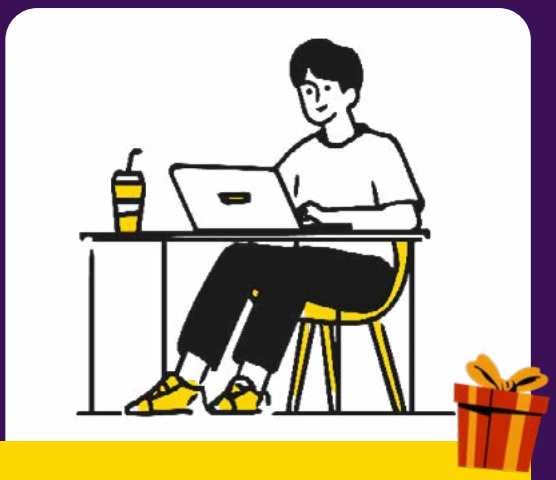
Digital Safety (DS) is an accredited IASME assessing body, supporting schools, trusts and suppliers through Cyber Essentials and Cyber Essentials Plus assessments.

Scan for 75% off

For further info scan the QR code above or email cyber-essentials@ds-cic.com

digitalsafety
DIGITAL SAFETY FOR ALL

ONLINE SAFETY NEWSLETTER



Staff Edition

"Helping Schools Build Safer, More Digitally Resilient Communities"

Barbara Spooner, MBE
CEO, Digital Safety CIC



"Every school deserves the confidence that its people, systems and pupils are protected in an increasingly digital world. That's why Digital Safety CIC exists - to provide practical support, trusted advice and expert guidance that makes a real difference." *Barbara Spooner MBE*

Supporting Your School

- Develop a whole-school digital safety strategy
- Prepare for the DfE Digital & Technology Standards
- Strengthen cyber security and online safeguarding
- Build staff confidence through practical training
- Support governors and senior leaders with strategic advice
- Help create a safer digital culture across your school

How We Can Support You

Whether you're looking to:

- improve cyber resilience
- strengthen online safeguarding
- understand new AI guidance
- support staff training
- prepare for future DfE requirements
- develop a long-term digital strategy

our team can provide practical support tailored to your school.

Find out more here



Gill from DS delivering to communities

WISHING YOU ALL A HAPPY & HEALTHY FESTIVE TIME!