Cotham School
Online Safety Newsletter

Academic Year: 2025/2026

Term: 1
Date: 03/09/2025

Newsletter Topic:
1. What is: The Online Safety Act (2023)
2. How to use: Virtual Private Networks (VPNs)

What is the UK Online Safety Act?

The UK Online Safety Act (2023) is a new law designed to make the internet safer for everyone — especially children. It places legal duties on social media platforms, search engines, and other online services to:

- Protect children from harmful and age-inappropriate content (e.g. pornography, violence, self-harm material)
- Remove illegal content quickly, including child sexual abuse material, terrorism, and online abuse.
- Enforce age limits using tools like age verification or estimation.
- Be transparent about risks and give users clear ways to report harmful content.
- Face penalties if they fail to comply — fines of up to £18 million or 10% of global turnover.

What this means for families:

- Platforms must take stronger action to keep children safe.
- Parents and children will have clearer reporting tools.
- Age checks will become more common on certain sites.

You can read the government's full explainer here.

Controversies about the Online Safety Act

The Act requires age verification for accessing adult or harmful content — often via ID scans, facial recognition, or credit card checks. Critics argue this invades privacy of adults also, forcing users to hand over sensitive data to third-party companies. Some platforms now require selfie-style verification just to access forums or music services. Some fear the Act could lead to over-censorship, where even legitimate content (e.g. political speech, technical forums) is blocked.

Proton VPN, an app offered by Swiss privacy tech firm Proton, has said it had seen a 1800% spike in UK daily sign-ups over the weekend after age check rules took effect.

Online habits of UK children (8–17) – An Ofcom report found that most UK children spend 2–5 hours online daily, and nearly all over the age of 12 own a mobile phone. Half of the participants said being online benefits their mental health.

What is a VPN — and Why Should Parents Know About It?

A VPN (Virtual Private Network) is a tool that hides a user's real location and encrypts their internet traffic. It can be useful for privacy — for example, when working remotely or using public Wi-Fi — but it can also be misused.

Why children might use VPNs?

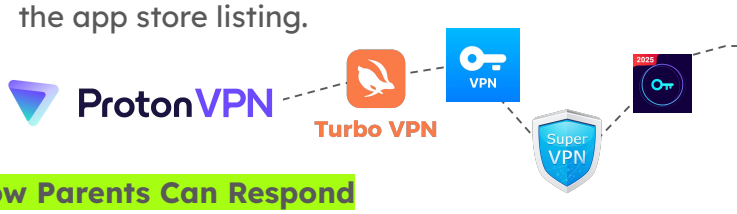
- To bypass parental controls or school filters.
- To access blocked websites or apps.
- To hide browsing activity.

Risks for children:

- Exposure to harmful, age-restricted content.
- Reduced visibility for parents and schools to monitor online safety.
- Some free VPNs carry malware or misuse personal data.

Signs your child may be using a VPN:

- Unknown apps with names like "Turbo VPN" or "Super VPN".
- App icons with cartoon animals, shields, or lightning bolts.
- No clear company name or privacy policy in the app store listing.



How Parents Can Respond

- Talk openly with your child about why they might want to use a VPN.
- Explain the risks — especially with free or unverified VPNs.
- Check devices for unfamiliar apps and review app permissions.
- Use parental controls to limit app installations.
- Model safe online behaviour and encourage children to come to you with concerns.

Useful Resources:

➔ NSPCC: What the Online Safety Act means
➔ Internet Matters: Guide to VPNs for parents

Cotham School
Online Safety Newsletter

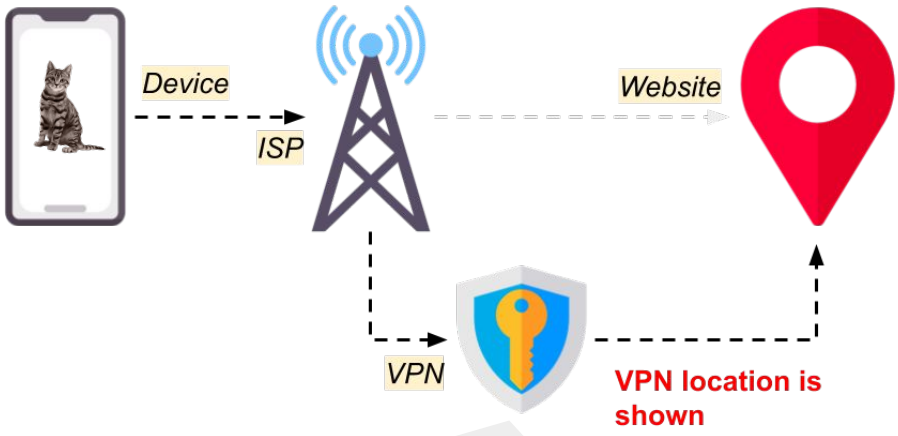
Academic Year: 2025/2026

Term: 1
Date: 03/09/2025

How VPNs Work:
A VPN routes internet activity through another server (often in another country). It hides a device's IP address so websites can't easily track location. It can also encrypt data so it is harder to intercept.

Without a VPN, devices connect to websites through an Internet Service Provider (ISP), which assigns a unique IP address to the device. This IP address is linked to the ISP and the user's approximate location. It is visible to websites, online services, and potentially third parties monitoring network traffic.

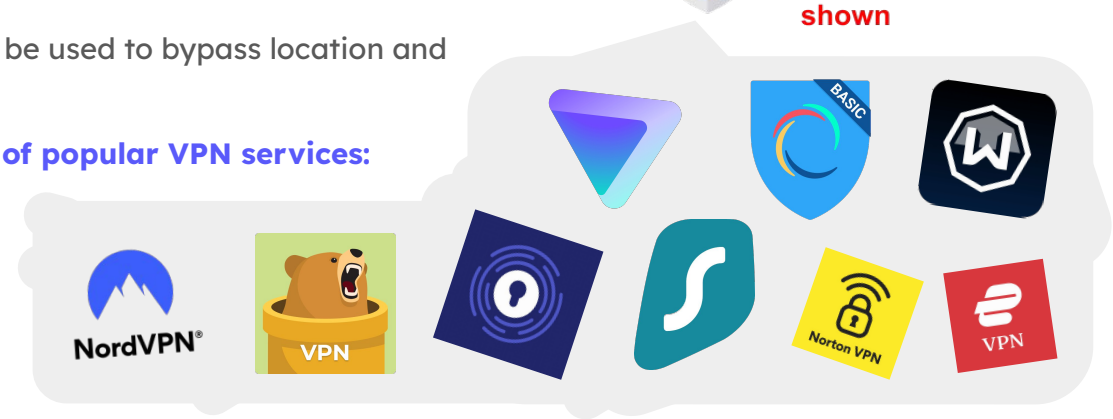
With a VPN, internet traffic is sent through a remote server operated by a VPN provider. This server hides the real IP address and replaces it with the IP address of the VPN server, effectively hiding your location and identity from websites and online services. The VPN also encrypts the activity of the user to add another layer of security.



This means that VPNs can be used to bypass location and age verification.

Here are some examples of popular VPN services:

- ProtonVPN
- TennelBear VPN
- ProvadoVPN
- NordVPN
- Surfshark
- Hotspot Shield



Accessing a VPN is pretty straightforward these days. Here's are some steps to access a VPN:

1. **Choose a VPN provider** – Pick a reputable service like NordVPN, ExpressVPN, or ProtonVPN. - Paid VPNs are generally safer than free ones (many free VPNs collect and sell data).
2. **Download the app** – Install the VPN software on your device (Windows, macOS, iOS, Android).
3. **Sign in** – Create an account, then use your credentials to log in.
4. **Connect to a server** – Select a location and tap "Connect". On Free VPNs, you may be automatically assigned a server. The VPN app will show a "Connected" status which indicated it is working. You can also check your IP address through whatismyip.com.
5. **Secure browsing** – The VPN now encrypts your traffic and hides your location; disconnect to return to your regular internet connection.