Llywodraeth Cymru
Welsh Government

A practitioner's guide to understanding risks of the dark web

Mae'r ddogfen yma hefyd ar gael yn Gymraeg.
This document is also available in Welsh.

OGL © Crown Copyright WG40568 Digital ISBN 978-1-80038-502-3

We hear about the dark web reported in the media in connection with online crime – but it's not a topic often covered in education. Discussing with learners how the dark web works, the reasons why people access it and the potential dangers is important – as this will empower learners to make informed choices when using the internet, positively and safely.

As a practitioner, it's important to balance the need to educate learners on the risks while avoiding 'glamorising' or promoting online tools and activities that could encourage illegal or harmful behaviour. At the same time, it should also be recognised that there are some legitimate legal uses for the deep and dark web, and these should be explained alongside the potential risks.

What is the dark web?

There are three main parts to the internet – the dark web being one:

1. **Surface (open) web** – is where all publicly viewable websites and content is found and indexed by search engines.

2. **Deep web** – accounts for 90 per cent of the internet hidden from conventional search engines. Users visit it, but only to access specific, encrypted or password-protected content that requires permission or payment in order to be viewed. The deep web also contains the 'back end' for banking, payments, forums and video on demand.

3. **Dark web** – refers to the part of the internet intentionally hidden from search engines. It uses masked IP addresses, and can only be accessed with a special web browser.

The deep and dark parts of the web contain a broad range of content. And while it's important for learners to understand that such sites exist, it is **highly unlikely** that they would need to visit them within the context of education. Indeed, schools should block such content in line with recommended filtering and monitoring requirements.

Who might use the dark web?

To effectively safeguard learners it is important to understand that it's possible for anyone to access the dark web by downloading a special web browser (Tor). Whilst there are some legitimate reasons for using the dark web by, for example, academics, journalists or activists, it has also become associated with illegal activity used by criminals and hackers.

Why do people use the dark web

- **Freedom from surveillance** – the dark web permits free exchange of and access to information for citizens in countries where the internet is censored or restricted.

- **Protection of freedom of speech** – users can connect with other dark web users regardless of their geographical location and share any opinion/viewpoint without fear of moderation or censorship.

- **Exposing abuses of power** – the dark web offers a space for journalists, activists and whistleblowers to report and discuss stories.

- **Greater anonymity** – limited personal information is automatically collected or stored by search engines or advertisers, and internet service providers (ISPs) cannot track browsing history.

- **It's possible to buy legal goods anonymously** – browsing and purchase history cannot be tracked by large internet companies such as Google or Amazon.

- **Access to illegal drugs** – around 57 per cent of dark activity is associated with trading in drugs (McGuires, *Into the web of profit*, 2018).

- **To purchase illegal items** – marketplaces hosted on the dark web may offer 'hidden services' where items such as firearms or drugs may be purchased.

What are the risks of using the dark web?

- **Illegal access** – browsing on the dark web is not illegal, but accessing illegal websites on the dark web using an anonymous browser, ***is***.

- **Criminal activity** – the anonymity and freedom the dark web affords has given rise to criminal activity, such as the sale of illegal or restricted products/services. These include drugs, dangerous substances, weapons/firearms, pornography and forms of gambling. The dark web poses a number of technological, ethical and moral issues for law enforcement when building a case against criminal behaviour.

- **Criminal/harmful behaviour** – while the dark web provides a space to discuss ideas and views, it also poses risks to society, ranging from extreme ideologies and radicalisation to terrorism. Extreme content related to hurtful and harmful behaviour (such as pro-self-harm, pro-eating disorders, pro-suicide) can also be found.

- **Child sexual abuse** – the dark web is home to websites that contain illegal child sexual abuse content (for example, pictures and videos) as well as forums and discussion boards frequented by groomers and paedophiles to discuss child sexual abuse methodologies. Sites that allow paid livestreaming and 'paid-to-order' child sexual abuse content are also hosted on the dark web.

- **Anonymity** – while anonymity can encourage freedom of expression, it can also result in more dangerous and harmful behaviour in users towards one another. This is because they may believe they are free of any legal consequences as it is harder for law enforcement to track or monitor activity.

What advice can you give children and young people?

- **Be aware of the law** – the law still applies, regardless of whether someone is on the dark web or the surface web. Help learners to become familiar with laws related to online behaviour, and remind them that these still hold true if criminal offences are committed on the dark web.

- **Consider the purpose** – some children and young people may be curious about using the dark web to see how it differs to using the surface web. Encourage learners to carefully consider why they may choose to use the dark web, the possible consequences, and whether they could instead achieve the same result on the surface web.

- **Recommend surface web alternatives** – some children and young people may wish to use the dark web because they feel it provides greater privacy and security. Helping them choose less risky alternatives that avoid the dark web (for example, using a virtual private network (VPN) and privacy controls on social media) could provide greater protection around their identity.

- **Offer support and help** – remind children and young people that they can always turn to you or another trusted adult if they ever experience anything online that makes them worried, uncomfortable or upset, regardless of whether it is found on the dark web or not. Make them aware of other sources of help and support such as Childline, Meic, CEOP and the Report Harmful Content website.

Other ways to help keep learners safe

- **Stay calm and be honest** – if you become aware of a child or young person using the dark web, don't assume they are doing anything illegal. Instead, have an open and honest discussion about the ways they are using it and the risks they may face. This might allow you to suggest safer alternatives.

- **Follow safeguarding procedures** – if you believe that a child or young person's online behaviour (on either the surface or dark web) is putting them or others at risk of harm then always follow your school's or organisation's safeguarding procedures and ensure that the Designated Safeguarding Person (DSP) is informed.

If you require any support, contact the **Professionals Online Safety Helpline** on 0844 381 4772 or helpline@saferinternet.org.uk

For more information, visit Keeping safe online on Hwb where you'll find a wide range of online safety resources which are available bilingually.