DIGINEWS

T1 Week 1

WELCOME TO OUR FIRST DIGINEWS FOR THIS ACADEMIC YEAR!

OUR ONLINE SAFETY CURRICULUM

Term 1: Our online safety theme this term is ‘Self-Image and Identity.’ We will be exploring how our offline and online identities are shaped and how media impacts on gender, stereotypes, and our emotions. We will discuss our own identities and how people represent themselves in different ways online whether this is real or edited and how this can affect our own behaviour.

ProjectEvolve

To support this, you can think about factors that make you, you & celebrate them! It may be hobbies, family…Ask your child to take a selfie to reflect their uniqueness!

How can a selfie posted online affect your future?

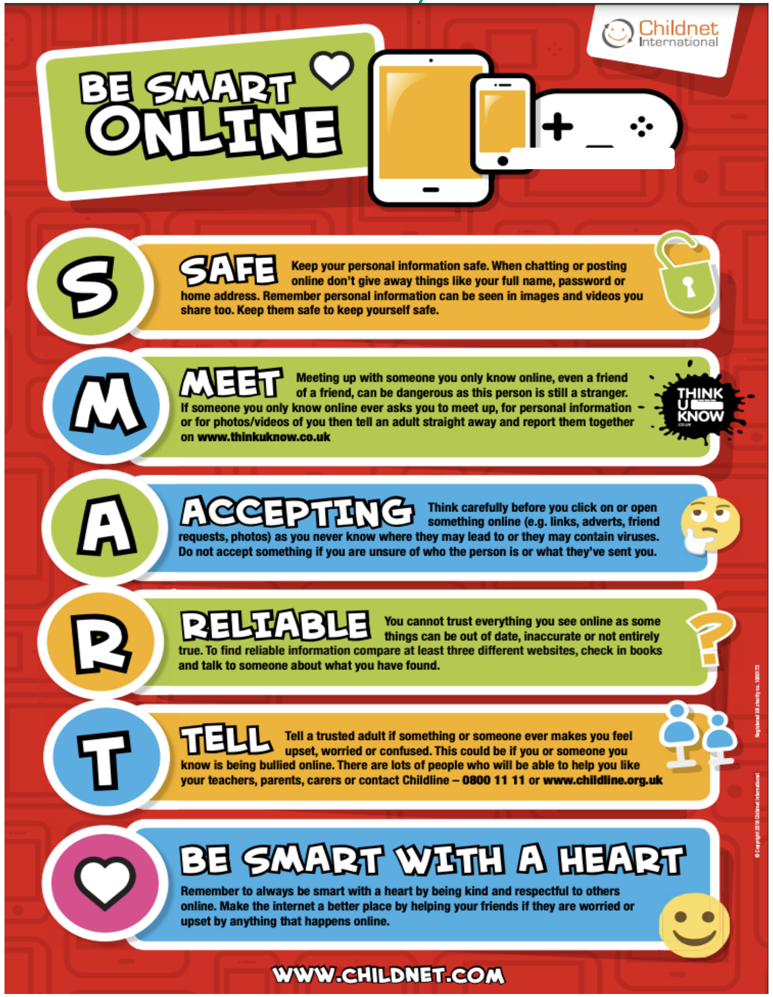
https://www.safesearchkids.com/online-safety-tips-for-kids-posting-pictures-online/

How do you feel about editing selfies?

If your child takes selfies, you may want to watch this:
https://www.bbc.com/ownit/its-personal/lauren-body-postiive

This term we will be focusing on the ‘S’ in our online safety SMART rules.

Talk to your child about what they understand this to represent. What do they know?



Childnet International

BE SMART ONLINE

S SAFE Keep your personal information safe. When chatting or posting online don’t give away things like your full name, password or home address. Remember personal information can be seen in images and videos you share too. Keep them safe to keep yourself safe.

M MEET Meeting up with someone you only know online, even a friend of a friend, can be dangerous as this person is still a stranger. If someone you only know online ever asks you to meet up, for personal information or for photos/videos of you then tell an adult straight away and report them together on www.thinkuknow.co.uk

A ACCEPTING Think carefully before you click on or open something online (e.g. links, adverts, friend requests, photos) as you never know where they may lead to or they may contain viruses. Do not accept something if you are unsure of who the person is or what they’ve sent you.

R RELIABLE You cannot trust everything you see online as some things can be out of date, inaccurate or not entirely true. To find reliable information compare at least three different websites, check in books and talk to someone about what you have found.

T TELL Tell a trusted adult if something or someone ever makes you feel upset, worried or confused. This could be if you or someone you know is being bullied online. There are lots of people who will be able to help you like your teachers, parents, carers or contact Childline – 0800 11 11 or www.childline.org.uk

BE SMART WITH A HEART Remember to always be smart with a heart by being kind and respectful to others online. Make the internet a better place by helping your friends if they are worried or upset by anything that happens online.

WWW.CHILDNET.COM

THINK U KNOW .co.uk
Registered UK charity no. 1080173
© Copyright 2018 Childnet International

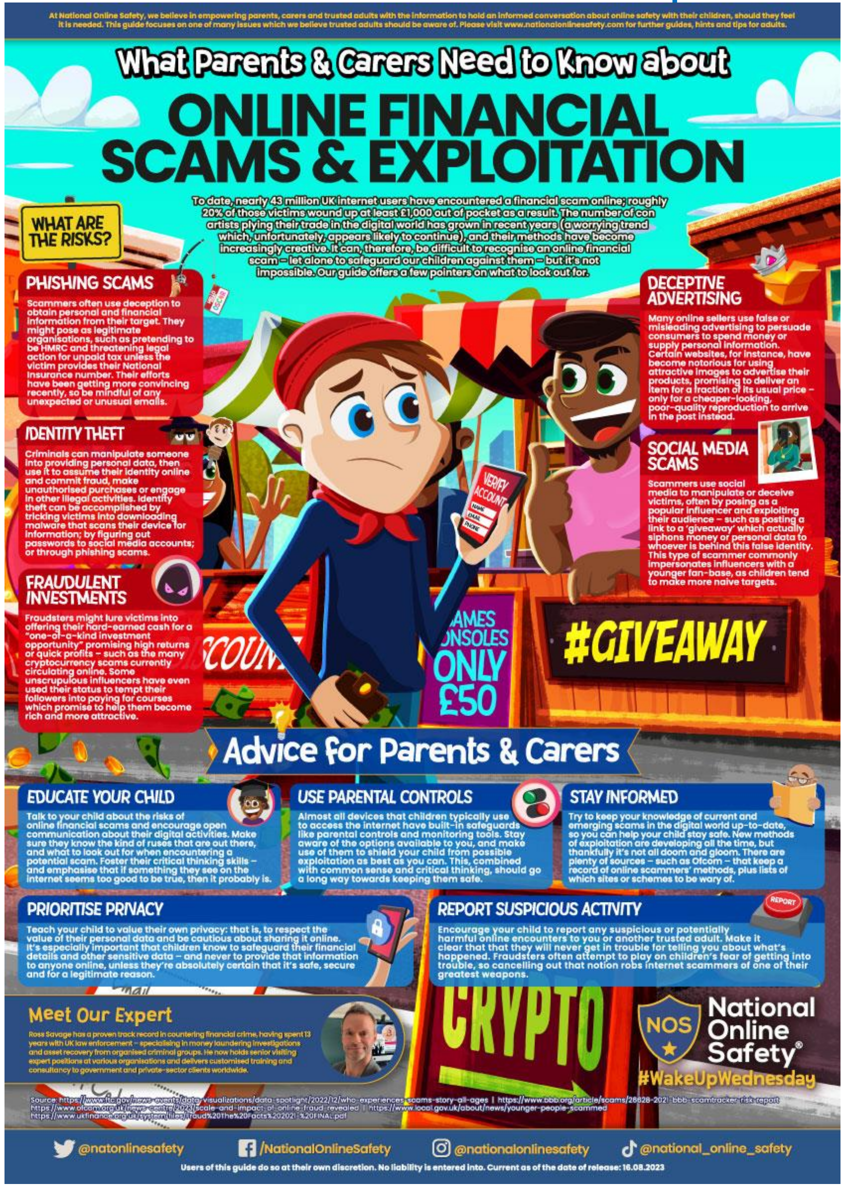
#EveryoneALearner

What makes us unique?

DIGINEWS

T1 Week 1

Some tips about technology from NOS…



At National Online Safety, we believe in empowering parents, carers and trusted adults with the information to hold an informed conversation about online safety with their children, should they feel it is needed. This guide focuses on one of many issues which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.

What Parents & Carers Need to Know about ONLINE FINANCIAL SCAMS & EXPLOITATION

To date, nearly 43 million UK internet users have encountered a financial scam online; roughly 20% of those victims wound up at least £1,000 out of pocket as a result. The number of con artists plying their trade in the digital world has grown in recent years (a worrying trend which, unfortunately, appears likely to continue), and their methods have become increasingly creative. It can, therefore, be difficult to recognise an online financial scam – let alone to safeguard our children against them – but it's not impossible. Our guide offers a few pointers on what to look out for.

WHAT ARE THE RISKS?

PHISHING SCAMS

Scammers often use deception to obtain personal and financial information from their target. They might pose as legitimate organisations, such as pretending to be HMRC and threatening legal action for unpaid tax unless the victim provides their National Insurance number. Their efforts have been getting more convincing recently, so be mindful of any unexpected or unusual emails.

IDENTITY THEFT

Criminals can manipulate someone into providing personal data, then use it to assume their identity online and commit fraud, make unauthorised purchases or engage in other illegal activities. Identity theft can be accomplished by tricking victims into downloading malware that scans their device for information; by figuring out passwords to social media accounts; or through phishing scams.

FRAUDULENT INVESTMENTS

Fraudsters might lure victims into offering their hard-earned cash for a "one-of-a-kind investment opportunity" promising high returns or quick profits – such as the many cryptocurrency scams currently circulating online. Some unscrupulous influencers have even used their status to tempt their followers into paying for courses which promise to help them become rich and more attractive.

DECEPTIVE ADVERTISING

Many online sellers use false or misleading advertising to persuade consumers to spend money or supply personal information. Certain websites, for instance, have become notorious for using attractive images to advertise their products, promising to deliver an item for a fraction of its usual price – only for a cheaper-looking, poor-quality reproduction to arrive in the post instead.

SOCIAL MEDIA SCAMS

Scammers use social media to manipulate or deceive victims, often by posing as a popular influencer and exploiting their audience – such as posting a link to a 'giveaway' which actually siphons money or personal data to whoever is behind this false identity. This type of scammer commonly impersonates influencers with a younger fan-base, as children tend to make more naive targets.

Advice for Parents & Carers

EDUCATE YOUR CHILD

Talk to your child about the risks of online financial scams and encourage open communication about their digital activities. Make sure they know the kind of ruses that are out there, and what to look out for when encountering a potential scam. Foster their critical thinking skills – and emphasise that if something they see on the internet seems too good to be true, then it probably is.

USE PARENTAL CONTROLS

Almost all devices that children typically use to access the internet have built-in safeguards like parental controls and monitoring tools. Stay aware of the options available to you, and make use of them to shield your child from possible exploitation as best as you can. This, combined with common sense and critical thinking, should go a long way towards keeping them safe.

STAY INFORMED

Try to keep your knowledge of current and emerging scams in the digital world up-to-date, so you can help your child stay safe. New methods of exploitation are developing all the time, but thankfully it's not all doom and gloom. There are plenty of sources – such as Ofcom – that keep a record of online scammers' methods, plus lists of which sites or schemes to be wary of.

PRIORITISE PRIVACY

Teach your child to value their own privacy: that is, to respect the value of their personal data and be cautious about sharing it online. It's especially important that children know to safeguard their financial details and other sensitive data – and never to provide that information to anyone online, unless they're absolutely certain that it's safe, secure and for a legitimate reason.

REPORT SUSPICIOUS ACTIVITY

Encourage your child to report any suspicious or potentially harmful online encounters to you or another trusted adult. Make it clear that that they will never get in trouble for telling you about what's happened. Fraudsters often attempt to play on children's fear of getting into trouble, so cancelling out that notion robs internet scammers of one of their greatest weapons.

Meet Our Expert

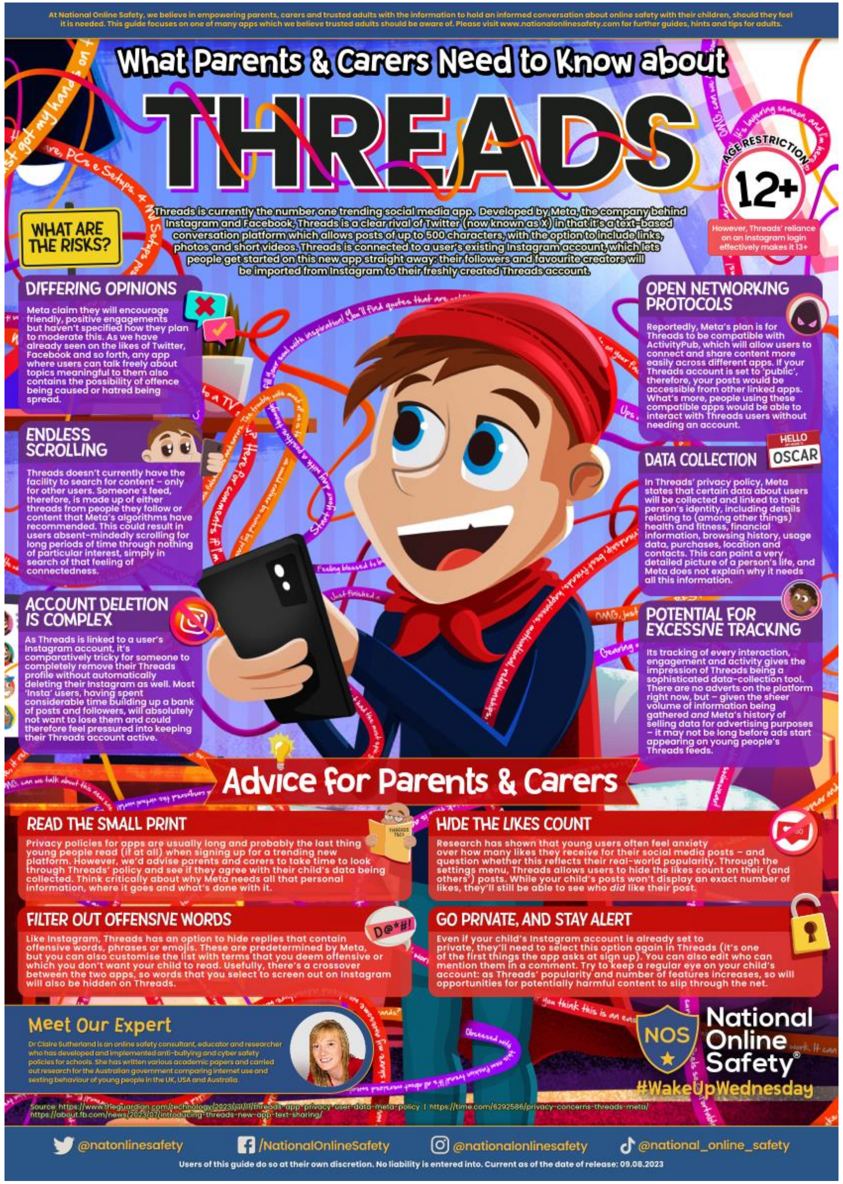
Ross Savage has a proven track record in countering financial crime, having spent 13 years with UK law enforcement – specialising in money laundering investigations and asset recovery from organised criminal groups. He now holds senior visiting expert positions at various organisations and delivers customised training and consultancy to government and private-sector clients worldwide.

NOS National Online Safety®
#WakeUpWednesday

Source: https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/12/who-experiences-scams-story-all-ages | https://www.bbb.org/article/scams/28628-2021-bbb-scamtracker-risk-report
https://www.ofcom.org.uk/news-centre/2023/scale-and-impact-of-online-fraud-revealed | https://www.local.gov.uk/about/news/younger-people-scammed
https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf

@natonlinesafety /NationalOnlineSafety @nationalonlinesafety @national_online_safety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 16.08.2023



At National Online Safety, we believe in empowering parents, carers and trusted adults with the information to hold an informed conversation about online safety with their children, should they feel it is needed. This guide focuses on one of many apps which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.

What Parents & Carers Need to Know about THREADS

AGE RESTRICTION 12+

However, Threads' reliance on an Instagram login effectively makes it 13+

Threads is currently the number one trending social media app. Developed by Meta, the company behind Instagram and Facebook, Threads is a clear rival of Twitter (now known as X) in that it's a text-based conversation platform which allows posts of up to 500 characters, with the option to include links, photos and short videos. Threads is connected to a user's existing Instagram account, which lets people get started on this new app straight away: their followers and favourite creators will be imported from Instagram to their freshly created Threads account.

WHAT ARE THE RISKS?

DIFFERING OPINIONS

Meta claim they will encourage friendly, positive engagements but haven't specified how they plan to moderate this. As we have already seen on the likes of Twitter, Facebook and so forth, any app where users can talk freely about topics meaningful to them also contains the possibility of offence being caused or hatred being spread.

ENDLESS SCROLLING

Threads doesn't currently have the facility to search for content – only for other users. Someone's feed, therefore, is made up of either threads from people they follow or content that Meta's algorithms have recommended. This could result in users absent-mindedly scrolling for long periods of time through nothing of particular interest, simply in search of that feeling of connectedness.

ACCOUNT DELETION IS COMPLEX

As Threads is linked to a user's Instagram account, it's comparatively tricky for someone to completely remove their Threads profile without automatically deleting their Instagram as well. Most 'Insta' users, having spent considerable time building up a bank of posts and followers, will absolutely not want to lose them and could therefore feel pressured into keeping their Threads account active.

OPEN NETWORKING PROTOCOLS

Reportedly, Meta's plan is for Threads to be compatible with ActivityPub, which will allow users to connect and share content more easily across different apps. If your Threads account is set to 'public', therefore, your posts would be accessible from other linked apps. What's more, people using these compatible apps would be able to interact with Threads users without needing an account.

DATA COLLECTION

In Threads' privacy policy, Meta states that certain data about users will be collected and linked to that person's identity, including details relating to (among other things) health and fitness, financial information, browsing history, usage data, purchases, location and contacts. This can paint a very detailed picture of a person's life, and Meta does not explain why it needs all this information.

POTENTIAL FOR EXCESSIVE TRACKING

Its tracking of every interaction, engagement and activity gives the impression of Threads being a sophisticated data-collection tool. There are no adverts on the platform right now, but – given the sheer volume of information being gathered *and* Meta's history of selling data for advertising purposes – it may not be long before ads start appearing on young people's Threads feeds.

Advice for Parents & Carers

READ THE SMALL PRINT

Privacy policies for apps are usually long and probably the last thing young people read (if at all) when signing up for a trending new platform. However, we'd advise parents and carers to take time to look through Threads' policy and see if they agree with their child's data being collected. Think critically about why Meta needs all that personal information, where it goes and what's done with it.

HIDE THE LIKES COUNT

Research has shown that young users often feel anxiety over how many likes they receive for their social media posts – and question whether this reflects their real-world popularity. Through the settings menu, Threads allows users to hide the likes count on their (and others') posts. While your child's posts won't display an exact number of likes, they'll still be able to see who *did* like their post.

FILTER OUT OFFENSIVE WORDS

Like Instagram, Threads has an option to hide replies that contain offensive words, phrases or emojis. These are predetermined by Meta, but you can also customise the list with terms that you deem offensive or which you don't want your child to read. Usefully, there's a crossover between the two apps, so words that you select to screen out on Instagram will also be hidden on Threads.

GO PRIVATE, AND STAY ALERT

Even if your child's Instagram account is already set to private, they'll need to select this option again in Threads (it's one of the first things the app asks at sign up). You can also edit who can mention them in a comment. Try to keep a regular eye on your child's account: as Threads' popularity and number of features increases, so will opportunities for potentially harmful content to slip through the net.

Meet Our Expert

Dr Claire Sutherland is an online safety consultant, educator and researcher who has developed and implemented anti-bullying and cyber safety policies for schools. She has written various academic papers and carried out research for the Australian government comparing internet use and sexting behaviour of young people in the UK, USA and Australia.

NOS National Online Safety®
#WakeUpWednesday

Source: https://www.theguardian.com/technology/2023/jul/11/threads-app-privacy-user-data-meta-policy | https://time.com/6292586/privacy-concerns-threads-meta/
https://about.fb.com/news/2023/07/introducing-threads-new-app-text-sharing/

@natonlinesafety /NationalOnlineSafety @nationalonlinesafety @national_online_safety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 09.08.2023

DIGINEWS

DOCS
SECRET
PICS
STORAGE FULL
100%
CONTACTS

At National Online Safety, we believe in empowering parents, carers and trusted adults with the information to hold an informed conversation about online safety with their children, should they feel it is needed. This guide focuses on one of many issues which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.

What Parents & Carers Need to Know about DATA BACKUPS AND STORAGE

Making backup copies of files and other content is very useful for avoiding issues (such as hardware failure, software problems or accidental deletion) that could cause the loss of important information or treasured images and videos. While backing up files is considered good practice, it's also essential for adults and children alike to stay aware of the risks which can potentially result from saving these extra copies of your info – particularly if your additional backup versions use cloud storage services.

BACKUP BASICS

Consider how valuable different types of files are – and what the impact would be if they were lost. Family photos and videos might be irreplaceable, for example, whereas emails to friends tend to be less important. This thought process can help you decide what to back up.

*For your most indispensable files, follow 'the 3-2-1 rule': keep **3** backups of your data (your original plus two copies) using **2** different media (such a USB flash, cloud storage or a hard disk drive) with **1** copy held in a physically separate location. This reduces the chance of a single event meaning that your files aren't recoverable from any of these backups.*

WHAT ARE THE RISKS?

DISAGREEABLE DUPLICATES

Because we tend to back files up in groups rather than individually, it's very easy for some content to get inadvertently swept up in the saving process – creating a duplicate that we aren't aware exists. If this were to include the unintentional backup of malware files, it would mean when we recover our data from the backup, we're also restoring the harmful malware to our computer, phone or tablet.

HIDDEN IN THE CLOUD

It's not unknown for children and young people to make use of cloud backup services to effectively 'hide' content that they know their parents and carers wouldn't approve of (such as something age inappropriate, for example). They can then delete the content from their device, safe in the knowledge that they can easily retrieve it from the cloud at a more convenient moment.

THE WEAKEST LINK

If any of our backups are insecure, then – in the event of a breach – the entirety of our data might become accessible to cyber criminals or other malicious individuals. Cyber criminals are aware that, by default, backups tend to contain important or valuable files that people want to keep safe – which makes them a popular (and potentially lucrative) target for cyber-attacks.

RANDOM RECOVERIES

When restoring data from one of our backups, we may find that some data is recovered which we hadn't even realised had been backed up. This doesn't necessarily sound like a huge drawback – but it could potentially cause a problem if the files were sensitive or personal in nature and then (without us realising) suddenly become available on our devices, where others might see them.

Advice for Parents & Carers

BE ORGANISED

Try to keep on top of what backups you and your children have in place – including where your files are saved (to the cloud or an external storage device, for instance) and how they can be accessed. It can also be helpful to stay aware of what data *isn't* being backed up, which could save you the time and the stress of looking for something in your backup that was never actually there.

KEEP THINGS TIDY

Where possible, curate your backups by learning how to add or remove content selectively. The former will save you from having to carry out a complete backup on every occasion (which can be time consuming), while being able to prune individual files can be extremely useful if a small number of unwanted – or possibly sensitive – items have been copied over and saved accidentally.

PRACTICE MAKES PERFECT

Find out how to recover files and information from backups until you're fully confident with the process. You could help your child practice with their own (or less essential) files, so they're able to restore items to their device if they need to. It's intensely frustrating knowing that your (or your child's) important files or cherished photo albums are there somewhere, but you can't get to them.

SCRUTINISE YOUR SECURITY

It sounds like obvious advice, but it's absolutely vital: ensure that your backups are secure. This includes appropriate technical measures – like encryption, strong passwords and multifactor authentication – and, where possible, physical security to prevent the media being stolen. If you're backing up to a hard drive or an external storage device, you should ideally use password protection.

Meet Our Expert

Gary Henderson is the Director of IT at a large boarding school in the UK, having previously taught in schools and colleges in Britain and the Middle East. With a particular interest in digital citizenship and cyber security, he believes it is essential that adults and children alike become more aware of the risks associated with technology, as well as the many benefits.

NOS National Online Safety®

#WakeUpWednesday

@natonlinesafety /NationalOnlineSafety @nationalonlinesafety @national_online_safety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 02.08.2023