

S VIRTUAL HOME LEARNING COMMUNITY

A youth leadership training programme empowering young people to educate their peers about online safety.



How to Create Student Digital Leaders and Establish a Virtual Home Learning Community

While teachers, carers and parents adapt to an alternative learn-from-home scenario, this new set-up will inevitably increase the amount of screen time children spend on their personal computers and devices. Because we don't know how long this situation will last for, we've combined a way to manage your students' time online and improve their internet savviness!

To support schools in teaching children the importance of online safety, we've devised a simple solution that teachers are going to love. Assign a small number of students online safety activities to complete, and encourage the successful participants to become special safety advocates or 'Digital Leaders'. Using what they've learned, these Digital Leaders will pass on their exclusive expertise to the rest of the student body.

With a virtual team of Digital Leaders managed by teachers, both schools and parents can feel more confident that their children will gain valuable insights from our unique, student-led approach to understanding online safety. Not only will this approach enhance awareness and responsibility amongst your students, it will bring a sense of community to remote learning.



Digital Leaders Explained...

We believe young people learn better from other young people. So, how can teachers create a virtual leadership team from their students? Our Digital Leaders pack contains all the information schools will need, like how to choose the right advocates, setting tasks, monitoring progress and even more.

We've devised a collection of activities, using guides, trivia, games and images, to make learning about online safety engaging, practical and useful. That's right - what better way to educate and entertain the curious minds of tomorrow?

With this newly acquired knowledge, your Digital Leaders can put what they've learned about online safety into practice - becoming an authority on the subject.

How does it work?

- O **Assign:** Teachers send the Online Safety Activity pack via email, Google Docs or school engagement app to a small number of young people they have chosen to become their Digital Leadership representatives.
- O Complete: The young people you've chosen will complete the activities and send them back to their teacher to be marked (via email).
- O **Teach:** Once checked, and depending on the answers, this will enable teachers to choose their Digital Leaders, who can then be tasked to virtually **teach** other young people what they have learned to their class which is ideal for establishing a learn-from-home community.
- O **Keep:** So they don't forget, Digital Leaders can **keep** the activities as a reference tool to help them retain the facts to pass on.

There are plenty of ways to get the message across, with virtual lessons and follow-up discussions via apps or social media community groups. Group or 1-2-1 chats can be conducted easily by following the <u>appropriate safeguarding advice outlined by the UK Safer Internet Centre</u>. Free platforms like Zoom, Google Hangouts Meets or Microsoft Teams are ideal platforms to keep up the conversation.



What's Included in this Online Safety Activity Pack

- ✓ Anti-Social Media! How to determine if a social media profile is genuine or not with spot the difference images
- ✓ Fake News Pop Quiz! Ten questions to test your children's knowledge on how to identify sources of fake news
- Can you Crack Cryptography? A cryptogram game to highlight the dangers of sharing private information





This is a headline you can trust and get excited about! But not all news is real or trustworthy. What makes it stand out is that it can look more interesting or outrageous than the real news - but there's a reason for that. 'Fake News' is intentionally designed to mislead, misinform and spread rumours.

For instance, there might be a catchy headline like, *Discover the secret to losing 20lb in 1 week!*, or *Find out what shocking thing Chris Hemsworth said at the Oscars*, and *Woman trains squirrel to scare her mother... and is arrested.* These are prime examples of 'clickbait' - attention - grabbing stories to make you click and get directed to a dodgy site.

False articles can also be shared across social media, so you can easily come across a hoax when you're checking social media. However, a <u>report from the National Literacy Trust</u> revealed some startling statistics:



2% of children can tell if a news story is real or fake.



The report also found that **49%** of young people are worried about **not being able to spot fake news**, both online and offline.

See? It's not easy to tell fact from fiction (adults find it difficult too!) And 50% of teachers that were surveyed felt that the national curriculum does not equip children with the right level of literacy skills to identify fake news either.



Take our quiz to find out if you can tell fact from fiction:

1.	Opinion pieces or personal blog posts are unreliable as accurate sources of news - and may even be false. A lack of is an obvious sign it is FAKE news. Fill in the blank: a) Margins b) Named quotes c) Paragraphs d) Celebrity interviews
2.	When in doubt, where should you check to make sure the website looks GENUINE? a) Homepage b) Other articles with similar headlines c) URL d) Click on other links on the same page
3.	If a news site doesn't have a, this is suspicious - don't trust it! Fill in the blank: a) Photo b) Logo c) Contact Us page d) Twitter post
4.	To determine if an article is TRUE, look at the type of message the article is trying to communicate. If there is it's genuine! Is the answer: a) The same news in multiple places b) No other news online c) No credible source online d) A range of "expert" quotes that don't match
5.	What is another word for the type of websites that can't be taken seriously because their purpose is to be funny or comical? a) Sitcom b) Superficial c) Sunshine d) Satirical



- 6. Fake news stories often have some kind of agenda to change opinions or persuade people to react to something. Which of these sensational story headlines is NOT a work of fiction:
 - a) The Prime Minister adopts alien baby
 - b) Town evacuated amid fears of the moon colliding with Earth
 - c) 94-year-old Harriette Thompson becomes oldest woman to run half marathon
 - d) Doctors discover incredible new pill to reverse the aging process
- 7. Did you know that even .com or .net website domains may not be entirely safe from fakers? Which of the following ones is definitely the LEAST credible?
 - a) .gov
 - b) .edu
 - c) .co
 - d) .org
- 8. If the story doesn't come from a media outlet you recognise (like BBC News, Metro.co.uk, etc.) or has a URL that doesn't seem to match the name of the website what else can you search for?
 - a) The author's name in Google or LinkedIn
 - b) Similar images using Google Image Search
 - c) If the website has recent news posts or if they're outdated
 - d) All of the above
- 9. Which of the following media outlets is NOT a reputable source for news coverage?
 - a) BBC News bbc.co.uk/news
 - b) Reuters uk.reuters.com
 - c) The Guardian theguardian.com/uk
 - d) NBC News nbcnews.com.co
- 10.Taken from a BBC News April Fools' Day 2017 post and BBC Radio 4's funniest news stories of 2018 - can you spot which unbelievable news story is actually FAKE? Go on, it's a difficult one...
 - a) "Missing woman unwittingly joins search party looking for herself"
 - b) "London's iconic Big Ben clock to go digital"
 - c) "Student discovers a massive Crunchy Nut cornflake"
 - d) "Sharks love jazz, say Australian scientists"

We hope you learned and laughed during the quiz! Find out your score from your teacher to see if you're a pro at spotting Fake News...



Here are the answers to the Fake News Quiz:

1. b) Named quotes

Why: A credible news story will include plenty of facts such as quotes from industry experts, reports, surveys and official statistics. If there isn't a sign of any one of these - or if the source is an "unknown", an "unnamed expert" or even a "friend" - investigate it. Also, question if the evidence proves that something definitely happened - or is it an extreme theory? If the facts, statistics and quotes have been twisted to conveniently support a specific point-of-view - question it's validity even more!

2. c) URL

Why: Fake news sites often mimic other credible or well-known sites, by copying the domain, logos and design. However, strange-sounding URLs that end in extensions like ".infonet", ".offer" or ".co" instead of ".gov", ".edu", ".net", ".com" or ".co.uk" are suspicious. Look out for domains with spelling errors too. If a website is trying to appear official, but the web address is weird, then this is a clue. E.g. If you were searching for the official Apple website but the URL was "www.appleproducts.org". Even if the URL doesn't appear to be dodgy, it could be full of fake news and advertorials.

3. c) Contact Us page

Why: If you're reading an article on a website you've never heard of before, take a look at the website's "Contact" and "About Us" pages. Fake news sites won't invest time in filling these sections in - and won't supply contact information to get in touch with them. If the site lacks these pages altogether, that's also a red flag, as most news outlets want their readers to be able to contact them and learn more about them.

For intentionally satirical sites, there will be some kind of disclaimer to advise the reader that any stories are meant to be comical and funny:

"The Onion uses invented names in all of its stories, except in cases where public figures are being satirized. Any other use of real names is accidental and coincidental. The Onion is not intended for readers under 18 years of age."

If you're still unsure, you can carry out a quick search on Google to see if the suspicious site has a reputation for publishing fake or misleading news.



4. a) The same news in multiple places

Why: If the story has been published by other well-known news media organisations like BBC News, CNN or Thomson Reuters, the facts will have been checked and verified. If the information you have isn't from a well-known source like these, there's a chance that it could be fake. Ensure you are checking the official sites and not websites that mimic the domains, logos and design...

5. d) Satirical

Why: News satire websites are a form of entertainment that are intended to be funny, comical and provocative. Each story is a spoof or parody of a real-life event, situation or celebrity in exaggerated circumstances. Fake news is misleading and tries to persuade the reader to react to the story that is a hoax. However, it can be difficult to distinguish between satire and fake news - as well as between satire and real news. Use the Fake News Checklist in the answer to question 8 below to help you.

6. c) 94-year-old Harriette Thompson becomes oldest woman to run half marathon

Why: This story has been checked online and appears in the Washington Post, Sports Illustrated, Runnersworld.com, CBS Philly, ESPN.com and more.

7. c).co

Why: The safest and credible website domains contain ".gov", ".edu" and ".org". Even ".com" and ".net" can be suspicious. Whereas official ".gov" sites or domains ending in ".edu" are more reliable and accurate sources of information. ".edu" domains are reserved for learning institutions, like colleges and universities, with studies and papers that have been written based on academic research and have been peer-to-peer reviewed.



8. d) All of the above

Why: Refer to your Fake News Checklist:

- Check the source Has an author's name been attached to the by-line and can you find them via a Google or LinkedIn search? If not it could be fake!
- See who else is reporting the story Can you find other credible media outlets, like BBC News, The Guardian, Thomson Reuters or Yahoo! News reporting the same story?
 If not - beware!
- Examine the evidence Is there a lack of quotes, comments with unnamed sources, a lack of 'About' or 'Contact Us' sections, strange looking website domains?
 Be cautious!
- Look for fake images Are the photos stock images or taken from other sites (check by right-clicking the image, save to your desktop, upload by clicking on the camera icon via Google Image Search) If yes - don't trust it!
- Determine if the story or website sounds right Check for spelling mistakes, grammatical errors, sensational headlines, a satirical tone, quotes from unknown sources that are conveniently used to support the point being made, the purpose of the story and if it's negative in nature. Investigate all tell-tale signs!

Check out the National Literacy Trust for more help and advice:

https://literacytrust.org.uk/policy-and-campaigns/all-party-parliamentary-group-literacy/fakenews/newsliteracy/

9. d) NBC News - nbcnews.com.co

Why: Even though NBC News is used as a trusted source, make sure the domain does not contain any suspicious characters, as fake news sites can mimic real URLs with a sneaky addition, like ".co" at the end. If there is a sequence of numbers at the beginning of a URL, this is a red flag for fake news domains too.

10. b) London's iconic Big Ben clock to go digital

Why: This is one of the many funny headlines featured in the BBC News April Fools' Day Quiz: https://www.bbc.com/ownit/the-basics/real-or-fake-news-quiz



Can You Crack Cryptography?

Privacy is paramount when you are online. You don't want to give away your personal information to someone you've never met, right? If you don't know who they are, what they want or how they're going to use your private details - it could be dangerous. Don't make it easy for cyberbullies and hackers to invade your privacy - there are simple ways to stop this from happening.

We've hidden 5 secret messages in the below 'cryptograms' - word puzzles, with messages that have been written in code. Each answer you reveal will make you think twice about how private you're being online and what to consider next time you log on...

In this activity, we've used numbers instead of letters. Take a look at the encryption key below:

Α	В	C	D	Е	F	G	Н	_	J	K	٦	М
1	2	3	4	5	6	7	8	9	10	11	12	13

N	0	Р	ď	R	S	Т	U	٧	W	Х	Υ	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

See how each letter is now linked to a number: A is 1, B is 2, C is 3, and so on..

To decrypt the hidden messages below, you'll need to use this secret key by matching the numbers to their corresponding letters. Each block of numbers is a new word and there is a hint to point you in the right direction.

Go on and get solving!



1st MESSAGE:

3		В	15	15	1	9	5
1							
12						, 1	
19	2	20	18	15	_	4	7
		4.5				4.5	
16	1	19	19	23	15	18	4

HINT: You'll need to do this when logging into any device (computer, phone or tablet) and for social media accounts too!

2ND MESSAGE:

4	4		15									
				<u></u>								
1	14		15		20	0						
16				15			19)		20		
16		18	9		2			1 20			5	
9	14	6	15	18	1	3	1	20	9	15	14	

HINT: Your date of birth, password and address...



3RD MESSAGE:

2		5	23	23 1			4		5
15		6]						
4	15	23	14	12	15	1	4	4	19

HINT: Don't get tricked into putting malware on your computer, which steals your private information and causes disruption.

4TH MESSAGE:

1				22		1	5		9		4		
19	19				1	1	8	9		14	7		
5	13		2	1	18	18	1	19	19	9 9	14	7	
19			5		12		6	9		5	19		

HINT: Any images (or mean messages too) can't be removed - even if you delete them once they've been posted.



5TH MESSAGE:

14			5		2	22			5		18	
3				8				1			20	
	20			15								
19	20)	18	1	1	4		7	5		18	19
15		1	4	12			9		14		5	

HINT: If you don't know or trust them, you shouldn't do this...

Don't stop there...

Why not make up your own hidden messages using the key above? Then try them out on your family and friends! Don't forget to use the answers you revealed in this activity to put into practice next time you're online...



How can you make sure your social media time is fun without worrying about the fake profiles? There are plenty of handy hints and tips to help you spot the difference between a friend and a phoney. These may be tricky at first - but you'll quickly get the hang of it when you put it into practice.

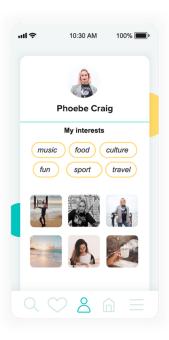
Look at our step-by-step guide for staying safe online (with some activities too!)...

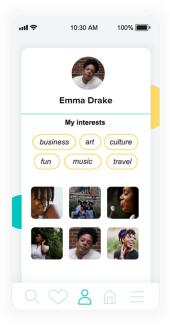
1. Investigate the profile image

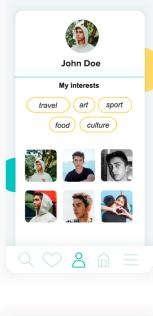
- O Is there only **one main image?** If you click on the profile pic and there are only one or two photos this is most likely an imposter. Compare this to how many photos you have in your album. There are dozens, if not hundreds, right? Real people typically change their profile pic every couple of months, especially if they go on holiday, have fun with friends or celebrate a special occasion.
- O Is there **no image** whatsoever? Whether it's a brand-new profile or if it has been created at least 2 years ago this could be fake. Don't risk it report and block it.
- O Are they using a **celebrity image**? It's not uncommon for someone to upload a main image of an actor, singer, celebrity or public figure. It tells you a bit about who they are and that they're a big fan of their work. But that is not always the case. The best way to confirm that the person is who they claim to be is to check the rest of their photos. If there aren't any other images excluding the celebrity ones it doesn't look good.
- Are they using **images of models?** If the pictures look like they've been lifted from an advert, catalogue, photo shoot or stock images you can do a bit of detective work using Google!
 - Simply right-click on the photo and then click on "Save image as..."
 - Save it to your Desktop
 - Next, click on Google Image Search (or type https://images.google.com into your web browser's address bar)
 - Choose the camera icon to "Search by image" and then click on "Upload an image"
 - Select the image from your desktop in the new window
 - Check the Google Image Search results to see if there are any duplicates or similar photos



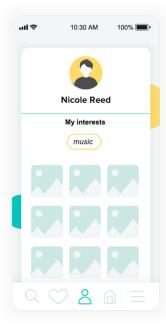
Now, can you spot the difference between these genuine and fake profiles below. All you need to do is circle the image that you think is a real profile:

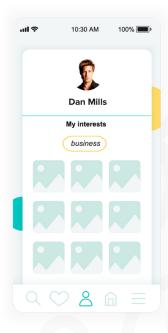


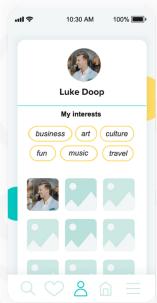




10:30 AM







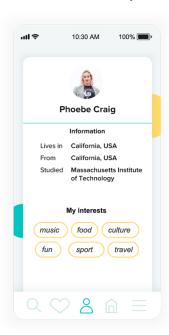


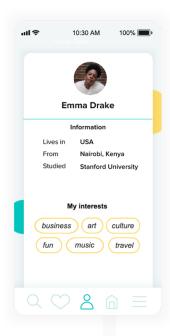
2. What's their About section about?

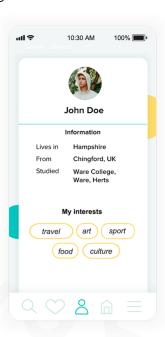
Who doesn't like to share (and brag a little bit!) about what they like, where they're from and the things they've done? It's only natural to want to talk about these things and show them off to your friends and family. What else would you put in your About section?

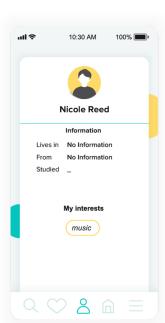
Well, if you're a social media faker, you're not a sharer. Not in the slightest. Therefore, if a profile only has information like where they live, where they work and where they studied this is a red flag. Especially if they just repeat the same place name. If it's too basic, don't buy it.

Now it's time to identify the fake from the for-real! Circle the right one below:

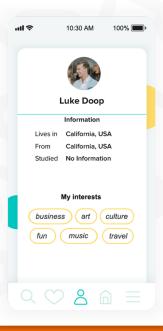










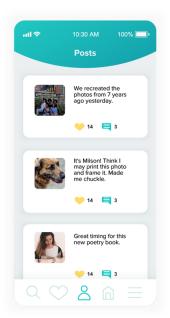


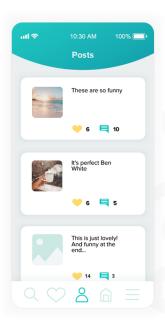


3. Check the Timeline activity

- O Are there lots of posts with links? Like with phishing scam emails, social media posts with links are a clear giveaway that this person is not genuine. If you notice that all they're posting is external links to "Check this out" then be wary. Don't trust a serial linker. If you click on an unknown link this could direct you to an untrusted site. Even if the link looks cool and is advertising a band or the latest smartphone, they could be trying to sell you something or get hold of your data.
- O Is there no activity or reaction to the posts? Dig deeper into the posts and see if there have been many comments posted by others. Fakes and phonies are not going to spend time liking and carrying on a conversation with replies even if they're positive. However, if there are posts, comments or replies by the suspicious user that don't make sense in context of the conversation, we recommend the block and report approach too.

Investigate further and highlight the images that display genuine profile activity:











What's Next

With new insights from the Online Safety Activity pack, your Digital Leaders will be confident in their new responsible role - teaching the rest of the class how to protect themselves online.

Once the safety activities are completed and checked - it's time for the next phase of the Digital Leadership programme to take effect:

- O Get your Digital Leaders to summarise what they learnt into a PowerPoint ready to share with each other
- O Talk it through with your class remotely using remote learning platforms such as Zoom, Google Classroom, Google Meet
- O Sign up to the Digital Leaders programme for more content and support

If you enjoyed the activity pack why not sign up to the Digital Leaders platform?

Get access to:

- Sample lessons for Primary and Secondary schools
- Discover how successful the Digital Leadership programme is working worldwide
- Access to our digital newsletters, keeping you up-to-date with the latest hints and tips

If you want to get access to more lesson plans and resources, begin your Digital Leadership journey and start earning badges. Simply click the button below to sign up, for free!

Start my Digital Leaders journey!