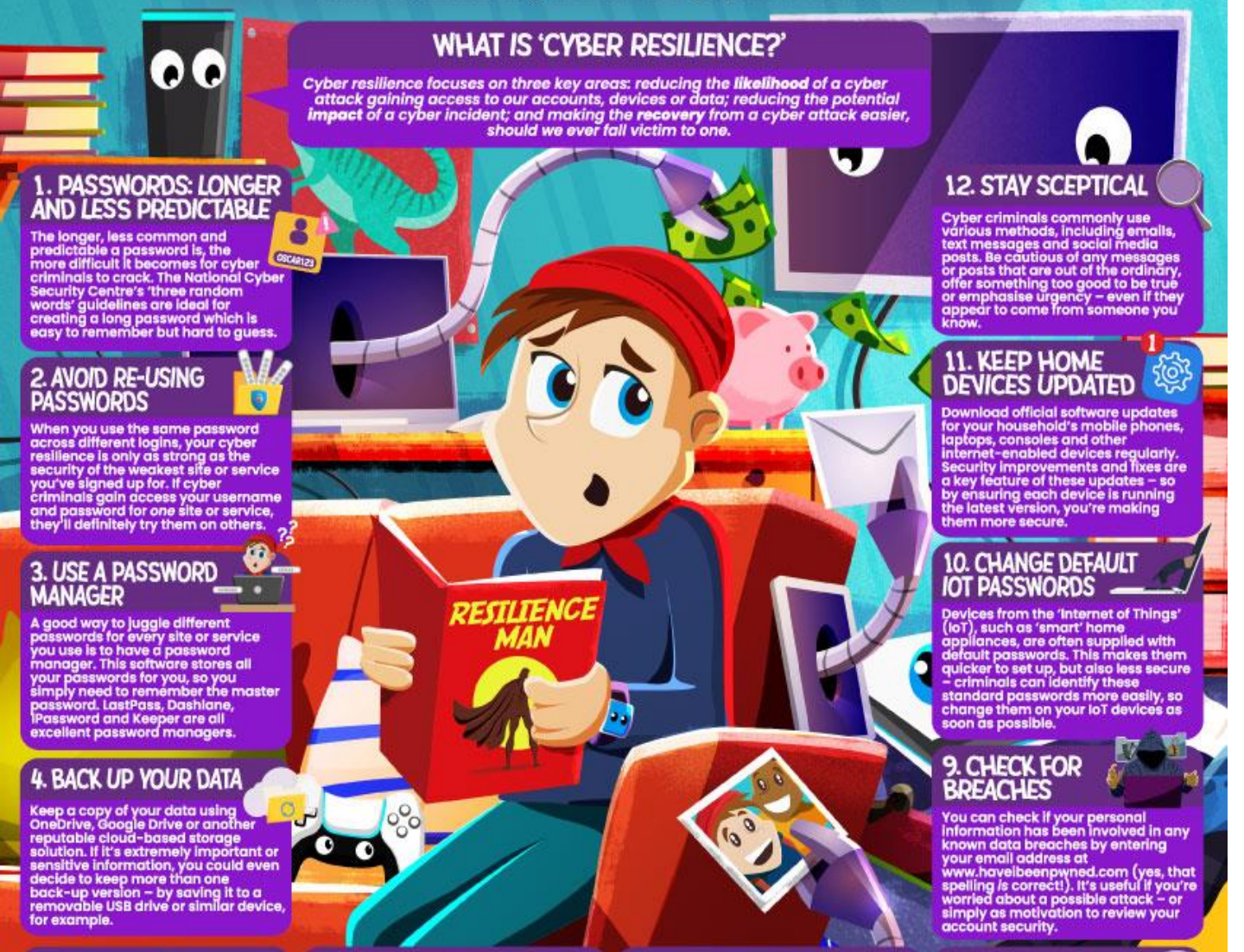
12 Top Tips for BUILDING CYBER RESILIENCE AT HOME

As a society, we're increasingly using technology and tech services in the home. Digital assistants which can adjust the heating or turn lights on and off; streaming services for shows and movies on demand; games consoles; smart speakers; phones; laptops ... the list goes on. As we introduce each new gizmo to our homes, however, we increase the level of threat from cyber criminals. It's essential, therefore, that we learn to become more cyber resilient in relation to the devices and digital services that the people in our household use.

WHAT IS 'CYBER RESILIENCE?'

*Cyber resilience focuses on three key areas: reducing the **likelihood** of a cyber attack gaining access to our accounts, devices or data; reducing the potential **impact** of a cyber incident; and making the **recovery** from a cyber attack easier, should we ever fall victim to one.*



1. PASSWORDS: LONGER AND LESS PREDICTABLE

The longer, less common and predictable a password is, the more difficult it becomes for cyber criminals to crack. The National Cyber Security Centre's 'three random words' guidelines are ideal for creating a long password which is easy to remember but hard to guess.

2. AVOID RE-USING PASSWORDS

When you use the same password across different logins, your cyber resilience is only as strong as the security of the weakest site or service you've signed up for. If cyber criminals gain access your username and password for *one* site or service, they'll definitely try them on others.

3. USE A PASSWORD MANAGER

A good way to juggle different passwords for every site or service you use is to have a password manager. This software stores all your passwords for you, so you simply need to remember the master password. LastPass, Dashlane, 1Password and Keeper are all excellent password managers.

4. BACK UP YOUR DATA

Keep a copy of your data using OneDrive, Google Drive or another reputable cloud-based storage solution. If it's extremely important or sensitive information, you could even decide to keep more than one back-up version – by saving it to a removable USB drive or similar device, for example.

5. ENABLE MULTI-FACTOR AUTHENTICATION (MFA)

Multi-factor authentication is where you need access to your phone (to receive a code, for example) or another source to confirm your identity. This makes it far more difficult for cyber criminals to gain entry to your accounts and your data, even if they *do* manage to get your username and password.

6. CHOOSE RECOVERY QUESTIONS WISELY

Some services let you set 'recovery questions' – such as your birthplace or a pet's name – in case you forget your password. Take care not to use information you might have mentioned (or are likely to in future) on social media. More unpredictable answers make cyber criminals' task far harder.

7. SET UP SECONDARY ACCOUNTS

Some services provide the facility to add secondary accounts, phone numbers and so on to help with potentially recovering your account. Make sure you set these up: they will be vital if you're having trouble logging in or if you're trying to take back control of your account after a cyber attack.

8. KEEP HAVING FUN WITH TECH

Consider our tips in relation to the gadgets and online services your household uses. Protect yourself and your family, and don't let the bad guys win: devices are not only integral to modern life but also a lot of fun – so as long as you keep safety and security in mind, don't stop enjoying your tech.

9. CHECK FOR BREACHES

You can check if your personal information has been involved in any known data breaches by entering your email address at www.haveibeenpwned.com (yes, that spelling *is* correct!). It's useful if you're worried about a possible attack – or simply as motivation to review your account security.

10. CHANGE DEFAULT IOT PASSWORDS

Devices from the 'Internet of Things' (IoT), such as 'smart' home appliances, are often supplied with default passwords. This makes them quicker to set up, but also less secure – criminals can identify these standard passwords more easily, so change them on your IoT devices as soon as possible.

11. KEEP HOME DEVICES UPDATED

Download official software updates for your household's mobile phones, laptops, consoles and other internet-enabled devices regularly. Security improvements and fixes are a key feature of these updates – so by ensuring each device is running the latest version, you're making them more secure.

12. STAY SCEPTICAL

Cyber criminals commonly use various methods, including emails, text messages and social media posts. Be cautious of any messages or posts that are out of the ordinary, offer something too good to be true or emphasise urgency – even if they appear to come from someone you know.

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.

National Online Safety®
#WakeUpWednesday

Source: www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-word | https://haveibeenpwned.com

Tips for Encouraging Open Discussions about DIGITAL LIVES

The online world is an entirely familiar and commonplace part of life for today's children and young people, far more so than for previous generations. There are many positives to children being able to access online materials, so it's important not to demonise the internet, games and apps, and limit the benefit of their positive aspects. At the same time, we *do* have a responsibility to educate children about the hazards they may encounter online (just as we would about real-world dangers) so it's essential that we don't shy away from talking to them about the complex – and often sensitive – subject of what they do and what they see when they're online.

Here are some suggestions for kicking off conversations with your child about their digital life ...

MAKE YOUR INTEREST CLEAR

Showing enthusiasm when you broach the subject signals to your child that you're keen to learn about the positives of their online world. Most children enjoy educating adults and will happily chat about what they use the internet for, or what games and apps they're into and how these work. Asking to see their favourite games and apps in action could help you spot any aspects that may need your attention – such as chat functions which might require a settings adjustment to limit contact with strangers. Keep listening even if your child pauses for a long time: they could be considering how to phrase something specific, or they may be gauging your reaction.

BE OPEN AND HONEST, APPROPRIATE TO THEIR AGE

At various stages, children and young people become curious about puberty and how their body changes; about relationships; about how babies are made; and about sexual health. If your child knows that they can discuss these sensitive subjects with you, they tend to be less likely to go looking online for answers – which can often provide them with misleading information and, in some cases, lead to them consuming harmful content. Don't worry if you don't immediately know the answers to their questions – just find out for yourself and go back to them once you have the facts.

REMIND YOUR CHILD THEY CAN ALWAYS TALK TO YOU

In my role I work with many children and young people who admit being reluctant to tell a trusted adult about harmful content they've viewed online, in case it leads to having their devices confiscated. Emphasise to your child that you're always there to listen and help; reassure them that if they *do* view harmful content, then they are not to blame – but talking about it openly will help. Children shouldn't be expected to be resilient against abuse or feel that it's their job to prevent it.

KEEP TALKING!

The most valuable advice we can give is to keep talking with your child about their digital lives. You could try using everyday situations to ask questions about their online experiences.

DISCUSS THAT NOT EVERYTHING WE SEE ONLINE IS REAL

Here, you could give examples from your own digital life of the online world versus reality – for example, those Instagram posts which show the perfect house: spotlessly clean, never messy and immaculately decorated. Explain to your child that there are many other aspects of the online world which are also deliberately presented in an unrealistic way for effect – such as someone's relationship, their body, having perfect skin and so on.

TRY TO REMAIN CALM

As much as possible, try to stay calm even if your child tells you about an online experience that makes you feel angry or fearful. Our immediate emotions frequently influence the way we talk, so it's possible that your initial reaction as a parent or carer could deter a child from speaking openly about what they've seen. Give yourself time to consider the right approach, and perhaps speak with other family members or school staff while you are considering your next steps.

CREATE A 'FAMILY AGREEMENT'

Involving your whole household in coming up with a family agreement about device use can be immensely beneficial. You could discuss when (and for how long) it's OK to use phones, tablets, consoles and so on at home; what parental controls are for and why they're important; and why it's good to talk to each other about things we've seen or experienced online (both good and bad). Explaining your reasoning will help children to understand that, as trusted adults, we want to make sure they are well informed and kept safe. Allowing children to have their say when coming up with your family agreement also makes them far more likely to stick to it in the long term.

Meet Our Expert

Rebecca Jennings of RAISE (Raising Awareness in Sex Education) has almost 20 years' experience delivering relationships and sex education and training to schools, colleges and other education providers. A published author on the subject, she also advises the Department of Education on the staff-training element of the RSHE curriculum.

National Online Safety®

#WakeUpWednesday

ONLINE CONTENT

10 tips to keep your children safe online

The internet has transformed the ability to access content. Many apps that children use are dependent on user-generated content which can encourage freedom of expression, imagination and creativity. However, due to the sheer volume uploaded every day, it can be difficult for platforms to regulate and moderate everything, which means that disturbing or distressing images, videos or audio clips can slip through the net. That's why we've created this guide to provide parents and carers with some useful tips on keeping children safe online.

1 MONITOR VIEWING HABITS

Whilst most apps have moderation tools, inappropriate content can still slip through the net.

2 CHECK ONLINE CONTENT

Understand what's being shared or what seems to be 'trending' at the moment.

3 CHECK AGE-RATINGS

Make sure they are old enough to use the app and meet the recommended age-limit.

4 CHANGE PRIVACY SETTINGS

Make accounts private and set content filters and parental controls where possible.

5 SPEND TIME ON THE APP

Get used to how apps work, what content is available and what your child likes to watch.

6 LET CHILDREN KNOW YOU'RE THERE

Ensure they know that there is support and advice available to them if they need it.

7 ENCOURAGE CRITICAL THINKING

Talk about what people might post online and why some posts could cause distress.

8 LEARN HOW TO REPORT & BLOCK

Always make sure that children know how to use the reporting tools on social media apps.

9 KEEP AN OPEN DIALOGUE

If a child sees distressing material online; listen to their concerns, empathise and offer reassurance.

10 SEEK FURTHER SUPPORT

If a child has been affected by something they've seen online, seek support from your school's safeguarding lead.

National Online Safety®

#WakeUpWednesday

10 Ways You Can SHARE KINDNESS ONLINE

Last year, around one in five young people aged 10–15 in England and Wales admitted experiencing online bullying: most commonly being insulted or sworn at, or having hurtful messages sent about them. To someone who's being bullied, the world can seem like a bleak, negative place – but just one kind word can be a ray of hope: a turning point that brightens their day and refreshes their perspective. That's why 'One Kind Word' is the theme of Anti-Bullying Week 2021. We're supporting this year's event by bringing you ten top tips for beating online bullying by replacing it with kindness.

1 PRAISE WHERE IT'S DUE

Sometimes a friend or relative might post online about something they're proud to have achieved: maybe an exam they've passed, a new skill they've learned or a task they've completed. Celebrate their hard work and determination by being kind enough to praise them for it publicly.

2 REACH OUT

It's not always easy to tell what kind of mood someone is in just from what they post online. Simply dropping somebody a message to say 'hi', to ask if they're OK or to tell them that you're thinking of them could totally make their day.

3 RECOMMEND FUN THINGS

If there's something you enjoy doing online – perhaps you play a particular game, or you've found a really cool site – share it with someone you think will enjoy it. Even recommending a film or TV show you think they'll like can bring a little happiness to someone who really needs it.

4 OFFER TO HELP

Sometimes you might see a friend or family member posting a question online or asking for help with something they can't do themselves. Don't just ignore it – if you can help, get in touch. Something that's difficult for them might be no trouble for you!

5 POST POSITIVELY

Lots of people seem to go online purely to complain about things or be negative. Just because you're communicating online (and not face to face) doesn't mean you can't be positive, though! Post about things that make you happy and that you're thankful for. It could brighten someone else's day.

6 SHOW YOUR APPRECIATION

If somebody that you know has done something positive or shown kindness themselves, go online and thank them with a message or a post. Expressing your gratitude costs nothing and showing someone that you appreciate them will really make them feel good.

7 BE UNDERSTANDING

Showing empathy towards others is an act of online kindness which often gets overlooked. If you notice that someone you know is upset, drop them a message. Sometimes people just need someone else to listen to them and understand their situation.

8 SHARE INSPIRATIONAL POSTS

When you see something online that inspires you or makes you feel happy, share it with people you know. A spot-on quotation, a beautiful photo or an uplifting video can lift someone's spirits and help them to feel better about life.

9 THINK BEFORE COMMENTING

Thinking before we act can be just as important as acting in the first place. Taking a second to consider what you're saying in advance could stop you from posting something negative, hurtful or offensive – even if you don't mean to. It's better to post positively or not post at all.

10 LIKE, LOVE AND ENGAGE

If somebody posts something that you like on social media, don't just scroll past – take the time to like it, love it or leave an appreciative comment! Reacting positively to other people's posts might seem like a small gesture but could mean a lot to them.

Meet Our Expert

Carly Page is an experienced technology journalist with more than 10 years of experience in the industry. Previously the editor of tech tabloid The Inquirer, Carly is now a freelance technology journalist, editor and consultant.

National Online Safety

#WakeUpWednesday

What Parents & Carers Need to Know about

HOW TO COMBAT ONLINE BULLYING

Defined as "ongoing hurtful behaviour towards someone online", cyber-bullying makes its victims feel upset, uncomfortable and unsafe. In the digital world, it has numerous forms – such as hurtful comments on a person's posts or profile; deliberately leaving them out of group chats; sharing embarrassing images or videos of someone; or spreading gossip about them. Cyber-bullying can severely impact a young person's mental health ... so, in support of Anti-Bullying Week, we've provided a list of tips to help trusted adults know what to look for and how to respond to it.

1. GET CONNECTED

Playing online games together with your child or connecting with them on social media (providing they're old enough) is not only fun but also an excellent way of establishing some common ground to discuss things you've both seen or done online – as well as keeping an eye on who your child is communicating with in the digital world.

2. KEEP TALKING

Regular chats with young people about their online lives are good practice in general, but they can also be an excellent refresher to help prevent cyber-bullying situations. Topics you might want to revisit include why it's important to only connect online with people we know and trust, and why passwords should always remain secret (even from our best friends).

3. STAY VIGILANT

Observe your child while they're using technology and just after they've used it. Are they acting normally, or out of character? Possible signs of a problem may include seeming quiet or withdrawn, jumpy or anxious, angry or repeatedly checking their phone. When you feel it's the right time, you may want to check in with them to see if everything is OK.

4. MAKE YOURSELF AVAILABLE

If an online bullying incident *does* occur, it may take a while before your child is ready to open up about what happened. Just gently remind them that they can always come to you with any problems – and that they won't be in trouble. You might also suggest a trusted family member they could turn to, in case they feel too embarrassed to tell you directly.

5. BE PREPARED TO LISTEN

When conversations about online bullying *do* take place, they're likely to be difficult, emotional and upsetting for both you and your child. Actively listen to your child while they're bringing you up to speed, and try not to show any judgement or criticism – even if they haven't dealt with the situation in exactly the way you would have hoped.

6. EMPOWER YOUR CHILD

Depending on their age, your child might not want a parent 'fighting their battles for them'. In that case, talk through their options with them (blocking the perpetrator, deleting the app and so on). By allowing your child to choose the path they take, you're putting them in control but are also demonstrating that you're there to support them along the way.

7. REPORT BULLIES ONLINE

Cyber-bullying often takes place through a particular app, social media platform or online game. If this is happening to your child, encourage them to report the offender to the app or game in question – ideally with screengrabs to support their complaint. Most games and apps have reporting tools specifically to stamp out abusive behaviour and protect users.

8. ENCOURAGE EMPATHY

Protecting themselves online is the priority, of course, but young people should also feel empowered to help if they witness other people falling victim to cyberbullying. Even if they don't feel confident enough to call someone out on their abusive behaviour online, they can still confidentially report that person to the app or game where the bullying occurred.

9. SEEK EXPERT ADVICE

Victims of online bullying frequently experience feelings of isolation and anxiety, a loss of self-esteem and potentially even thoughts of self-harm or suicide. If you think that an incident of cyber-bullying has affected your child's mental wellbeing, then seek psychological support for them. There are some useful contact details in the central panel below.

10. INVOLVE THE AUTHORITIES

If the nature of any online bullying makes you suspect that your child is genuinely in imminent physical danger – or if there are any signs whatsoever of explicit images being shared as part of the bullying – then you should gather any relevant screenshots as evidence and report the incidents to your local police force.

FURTHER SUPPORT AND ADVICE

If you or your child need additional help with an online bullying issue, here are some specialist organisations that you could reach out to.

Childline: talk to a trained counsellor on 0800 1111 or online at www.childline.org.uk/get-support/

National Bullying Helpline: counsellors are available on 0845 225 5787 or by visiting www.nationalbullyinghelpline.co.uk/cyberbullying.html

The NSPCC: the children's charity has a guide to the signs of bullying at www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/bullying-and-cyberbullying/ and can be reached on 0808 800 5000

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.

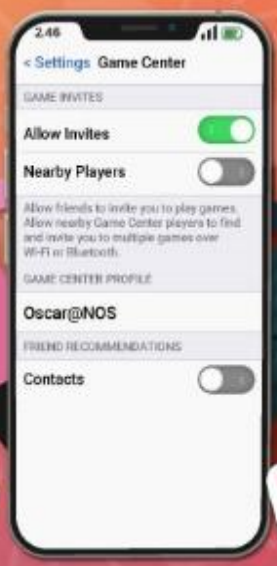
National Online Safety®

#WakeUpWednesday

How to Set up PARENTAL CONTROLS for APPS

iPhone

Apple devices come with built-in apps already available: Mail, FaceTime and Safari, for example. However, you can choose which apps and features appear on your child's device and which ones don't. You can also manipulate the features in Game Centre to enhance your child's safety and privacy when playing games, as well as blocking iTunes or App Store purchases if you wish.



How to Restrict Built-in Apps/Features

1. Open Settings
2. Tap Screen Time
3. Tap Content & Privacy Restrictions
4. Tap Allowed Apps (you may need to toggle this to 'on' at the top)
5. Enable or disable the apps you wish to appear (or disappear) on your child's device

How to Restrict Game Centre

1. Open Settings
2. Tap Screen Time
3. Tap Content & Privacy Restrictions
4. Tap Content Restrictions (you may need to switch the toggle at the top to the 'on' position)
5. Scroll down to Game Centre
6. Choose between Allow, Don't Allow, or Allow with Friends Only in the settings for each feature

How to Restrict iTunes & App Store Purchases

1. Open Settings
2. Tap Screen Time
3. Tap Content & Privacy Restrictions
4. Tap iTunes & App Store Purchases
5. Select Allow or Don't Allow for each feature (you can also lock these settings with a password)

National Online Safety®
www.nationalonlinesafety.com

ONLINE CONTENT

10 tips to keep your children safe online

The internet has transformed the ability to access content. Many apps that children use are dependent on user-generated content which can encourage freedom of expression, imagination and creativity. However, due to the sheer volume uploaded every day, it can be difficult for platforms to regulate and moderate everything, which means that disturbing or distressing images, videos or audio clips can slip through the net. That's why we've created this guide to provide parents and carers with some useful tips on keeping children safe online.

1 MONITOR VIEWING HABITS

Whilst most apps have moderation tools, inappropriate content can still slip through the net.

2 CHECK ONLINE CONTENT

Understand what's being shared or what seems to be 'trending' at the moment.

3 CHECK AGE-RATINGS

Make sure they are old enough to use the app and meet the recommended age-limit.

4 CHANGE PRIVACY SETTINGS

Make accounts private and set content filters and parental controls where possible.

5 SPEND TIME ON THE APP

Get used to how apps work, what content is available and what your child likes to watch.

6 LET CHILDREN KNOW YOU'RE THERE

Ensure they know that there is support and advice available to them if they need it.

7 ENCOURAGE CRITICAL THINKING

Talk about what people might post online and why some posts could cause distress.

8 LEARN HOW TO REPORT & BLOCK

Always make sure that children know how to use the reporting tools on social media apps.

9 KEEP AN OPEN DIALOGUE

If a child sees distressing material online; listen to their concerns, empathise and offer reassurance.

10 SEEK FURTHER SUPPORT

If a child has been affected by something they've seen online, seek support from your school's safeguarding lead.

National Online Safety®

#WakeUpWednesday

10 Top Tips for ...

KEEPING CHILDREN SAFE FROM CYBER CRIME

We all want to continue being informed and inspired by the ever-expanding capabilities of the internet. But we also need to be able to safeguard ourselves against the growing amount of online hazards. Knowing what is fact, understanding what dangers exist and taking appropriate steps can go a long way towards protecting yourself and your family. National Online Safety has collaborated with the Yorkshire and Humber Regional Cyber Crime Unit to compile 10 pointers to help you keep your children safe from cyber crime.

1. Spot Phishing Bait

Phishing messages are untargeted mass emails asking for sensitive information (e.g. usernames, passwords, bank details) or encouraging recipients to visit a fake website. It's safest to learn the warning signs of phishing and increase your child's awareness. Too good to be true? Spelling or punctuation errors? Odd sense of urgency? These are all red flags. Don't click on links or follow demands: if you're unsure, contact the official company directly online to enquire further.

2. Don't Over-Share

Is your child sharing too much on social media? Do they post things about their private life, upload images of your home, or discuss their friendships and relationships online? Criminals will gather this information and may try to use it for identity theft or other offences such as fraud. To combat this, ensure your child's privacy settings mean they are only sharing information with family and close friends. Use parental controls where appropriate.

3. Encourage Strong Passwords

Weak passwords make it faster and easier for someone to gain access to your online accounts or get control of your device – giving them a route to your personal information. For a strong password, national guidance recommends using three random words (e.g. bottlegaragepylons). Consider paying for your child to access a password manager. Encourage them to have a separate password for their email account. Ensure the whole family uses two-factor authentication where possible.

4. Stay Updated

People often put off installing updates to apps or software because they don't feel it's necessary, it can be time consuming, or could cause problems with programmes they rely on. But updates help protect users from recently discovered vulnerabilities to malware. You can usually set them to run automatically – encourage your child to select this option. Ensure updates are installed as soon as possible after you're notified they're available.

5. Back up Your Data

Some cyber attacks can lead to the theft or deletion of important (and possibly sensitive) data or loss of files (like photos and videos) that can't be replaced. Backing up your data to the cloud – or to another device – will help prevent data loss if you ever became the victim of a cyber attack. Where possible, set your child's devices to back up automatically. Also encourage them to back up their data prior to installing any updates.

6. Be Wary of Public WiFi

Free public WiFi is commonplace – but it's often not secure and sends unencrypted data via the network. A hacker on the same network could access personal data (like financial information) without you even realising they'd done so. To avoid this, suggest to your child that they use their 3G or 4G mobile data when they're out and about, rather than free WiFi. Consider purchasing a VPN (Virtual Private Network) where possible.

7. Take Care When Chatting

Criminals may look to manipulate others online and coerce them into using their talents or cyber skills for unethical means. Try to get your child to be open about who they are talking to online. Communication tools such as Discord are popular among gamers – but be cautious of the other people using them, and ensure you know who your child is chatting with.

8. Recognise Warning Signs

Often, budding cyber experts will relish the challenge of testing themselves or earning recognition from peers for their exploits. Even principled 'white-hat' hackers will look to test their skills online. If you think your child is interested in hacking, try to understand what their motivation is. You could encourage their participation in ethical competitions such as bug bounties.

9. Understand Their Motivations

Those being influenced online to use their skills unethically may display certain key warning signs. Sudden evidence of new-found wealth (unexplained new clothes or devices, for example), secrecy around their online behaviour or boasting of new online friendships are all causes for concern. If in doubt, refer through to your regional cyber crime team.

10. Know the Consequences

Many young people may feel that hacking is essentially a light-hearted prank, and not especially serious. So make sure your child is aware of the implications of a conviction under the Computer Misuse Act – not only the possibility of a criminal record, but also lifelong travel restrictions and damage to their future career or educational prospects.

Produced in Partnership with

The Yorkshire & Humber Regional Cyber Crime Unit (YHRCCU) works with the National Crime Agency (NCA) and other partners, in the UK and abroad, to investigate and prevent the most serious cyber crime offences.

YH ROCU

Yorkshire & Humber
REGIONAL CYBER CRIME UNIT

National Online Safety®
#WakeUpWednesday

What Parents & Carers Need to Know about

SHARING PHOTOS ONLINE

School is often a time chock-full of milestones for your child, and you may well be eager to share their accomplishments with the world. In today's digital age, sharing images of such precious moments on social media is commonplace, and – while that's a lovely thing to do – it *does* come with some risks attached. Our guide can help parents and carers to consider the potential dangers and make informed choices about safely sharing photos of their children online.

WHAT ARE THE RISKS?

INVASIONS OF PRIVACY

Even with the right settings in place, absolutely nothing online is 100% private. Anyone who can view your photos could take screenshots and potentially share them elsewhere. Privacy settings are still important, though, so it's always wise to ensure your social media accounts have them set up; just bear in mind that you can't *completely* control what happens to anything once it's gone online.

REVEALING PERSONAL DETAILS

Small details in photos can often reveal personal information. Backgrounds can give clues to where you live, for example, while school logos on uniforms, sports kits, or bags could help someone identify which school your child attends. With interactive maps and reverse image searches commonplace online, information like this could easily be misused by an individual with malicious intentions.

MISUSE OF IMAGES

Once something's been shared online, it's almost impossible to get it deleted. Photos can show up in search engine results and be downloaded, manipulated, and shared without consent. There's the potential for someone's images to be used for advertising purposes (which in many cases, isn't illegal) or even more inappropriate reasons, such as cyber-bullying or serious forms of exploitation.

ONLINE GROOMING

hi...

Pictures that convey details about your child's interests, activities, or daily routines could arm an online predator with the kind of information they can deploy to gain a child's trust. They might use this knowledge to pretend to be the same age as the child or to have a shared hobby. Essentially, the more a predator knows about a young person, the easier it is for them to invent some 'common ground'.

PRESSURE TO PLEASE

When their parents or carers share notable moments and accomplishments in a child's life on social media, some children may begin to feel an expectation to *always* meet certain standards, to achieve things, or to behave in ways that are "worth sharing". Knowing that other people (even friends and family) can see these posts on social media might also add to the pressure they're feeling internally.

IMPACT ON DIGITAL FOOTPRINT

Every photo of a child posted online contributes to their digital footprint. Young people's lives have never been so closely and publicly documented as they are now, and this permanent online presence could affect a child's future opportunities or the choices they make as they grow up – in addition to influencing how they see themselves and, consequently, their emotional wellbeing.

#backtoschool

Advice for Parents & Carers

REVIEW SETTINGS REGULARLY

Make sure your social media's secure in terms of who can view your content or see your location (only family and trusted friends, for example). Privacy settings aren't totally foolproof, but they *do* make it tougher for strangers to access your pics. Reviewing your settings regularly is also a good starting point for conversations with your child about managing their own social accounts when they're older.

CHECK YOUR PHOTOS

Photos of your child shouldn't provide any clues to where they live or go to school: even a house number, street name, or car number plate could be a giveaway. Cover up or blur out school logos, too. If you *really* want to share a particular pic, you could post a watermarked or low-res version, which can help to discourage misuse as those images are less appealing to download or reproduce.

CONSIDER OTHER CHILDREN

When taking a group photo, make sure you get parents' or carers' permission to share it on social media. There may be an important safeguarding reason for them not wanting their child's photo posted publicly online, or it might simply not tally with their personal beliefs or cultural background. A quick conversation in advance, just to make sure, is usually hugely appreciated.

THINK AHEAD

Try to consider the longer-term implications of what you post. Would you be happy with that photo being online in 10 years' time? Would your child still be OK with the image when they're older? Once your child is mature enough, you could ask for their consent before posting: it respects their privacy, fosters trust and understanding, and helps them to start thinking about their own online life.

Meet Our Expert

Gabriella Russo is a safeguarding consultant with more than 30 years' experience working with children, families, and adults in education, local authority, and mental health settings, both in the UK and internationally. She has developed online safety training for local authorities and foster care agencies across Britain and is the online safety expert for FosterWiki.

National Online Safety®

#WakeUpWednesday

@natonlinesafety /NationalOnlineSafety @nationalonlinesafety @national_online_safety

What Parents & Educators Need to Know about SHOPPING PLATFORMS

For people looking to make purchases on their phones, several shopping apps – such as Temu – allow users to buy goods at reduced prices. Others, like Vinted and Depop, let you sell items you no longer want. As internet shopping continues to grow, however, so does the risk of scammers, hackers and breaches of privacy.

WHAT ARE THE RISKS?

MISSING ITEMS

Users of Vinted, Depop and Temu have reported not receiving their products despite payment being taken. Users can initially contact the seller to query a missing item, and they have between two and five days (depending on the app) to tell the company what has happened. However, once the money has reached the supposed 'seller', it can be quite difficult to get back.

SCAMMERS AND PHISHING

Scammers are always on the lookout for unsuspecting buyers or sellers. Common tactics include cancelling shipment of an item once the payment has been processed or asking to conclude the chat and payment outside of the app, where the victim is no longer protected by the buyer protection plan. This should, naturally, be avoided at all costs.

DATA MISUSE

Apps of all kinds frequently collect our data, often asking for more information than is necessary to set up an account. Data gathered in this way is then usually sold on to third parties for marketing purposes. Lately, certain apps have been under scrutiny for using spyware to track their members' activities – but all too often, the user's consent to this practice has been hidden away in the terms and conditions.

FAKES OR REPLICAS

It's certainly not unheard of for poor-quality products to be falsely marketed as luxury items, using misleading pictures or clever wording. These disingenuous sales are sometimes outed by suspiciously low price tags, but this isn't always the case. For children and young people especially, there's a risk that the promise of bagging a high-end item for a fraction of its usual price will outshine any suspicions they may have.

SLOW REFUNDS

While all apps offer a refund if the product is damaged or doesn't match the description, it can take up to a month to be compensated for this. For many people (especially during a cost-of-living crisis) that can be a long time to be without both the product you bought *and* the hard-earned cash you spent on it.

MISLEADING DESCRIPTION

Some people will be able to notice when, say, a product's photo and its description don't seem to match. This isn't a reliable means of picking up on misleading marketing, however – especially not for children and young people, many of whom may not yet realise that such practises even exist. While it's illegal to advertise one thing and sell another, plenty of shady traders use clever wording and omissions to get around this.

Advice for Parents & Educators

ALWAYS STAY ON THE APP

It's vital that users pay for any goods through the same app on which they found them, to ensure they are covered by buyer protection. This means users can access support if the item arrives damaged, isn't as described, or doesn't arrive at all – allowing them to seek compensation for the loss. Such regulations can't protect you, however, if you didn't do the deal through the app in question.

CHECK REVIEWS

Take time to read the reviews and comments left by other users – not just of products, but of sellers and buyers, to ensure they're legitimate and reliable. Before buying an item online, check the reviews for comments about the product's quality, the seller's communication and the delivery time. If you're selling, check the reviews of your buyer for red flags such as frequent requests for refunds or claims of 'missing' items.

BE WARY OF PHISHING ATTEMPTS

Scammers frequently send messages within these apps to steal personal and financial information from other users. Don't respond to these messages – and under no circumstances should you follow any links they contain. Check for spelling errors, as well as inspecting the name of the sender. Report any suspected phishing emails to the app's help centre – and notify your bank if you think your financial information has been compromised.

KEEP SAFE AS A SELLER

Sellers can be exploited just as much as buyers. Some users may purchase an item, for example, then pretend it didn't arrive to secure a refund. Always take photos of the shipping label, along with a picture of you posting the item. Send the package's tracking number to the buyer and keep a copy for yourself, letting you investigate any future claims that it never arrived. When taking photos of items you're selling, ensure nothing personal is in the background.

Meet Our Expert

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

Source: See full reference list on guide page at: nationalcollege.com/guides/shopping-apps

#WakeUpWednesday®

The National College®

Part of our Online Mental Health & Wellbeing Series

NOS Online Mental Health & Wellbeing

Brought to you by National Online Safety®

www.nationalonlinesafety.com

What you need to know about...

AGE RATINGS

What are they?

'Age Ratings'

A game's age rating can be used by adults to make an informed choice as to whether or not a game is suitable for their child. The PEGI (Pan European Game Information) system rates games and, instead of indicating the level of ability required to physically play a game, it indicates the suitability of content for that age group. 3, 7, 12, 16 and 18 are the labels that can be awarded to games and a variety of content descriptors such as violence, bad language and fear are used to further clarify why the label was assigned.

Know the Risks

Inappropriate content

The biggest and most obvious risk of not following the age rating system is that children may view or hear age-inappropriate content. Many games now include scenes of a violent or graphic nature which could be upsetting or considered too intense for younger players.

Peer pressure

Peer pressure has a large role to play in age ratings being overlooked. Children don't want to be the ones left behind and can put their parents under pressure to allow them to play a game beyond the recommended suitability, especially when all of their friends are playing it already.

Level of 'Kudos'

Playing a game with a label that is higher than their age can be viewed by some children as a challenge and to gain a good reputation amongst friends. Kudos is attributed to the child playing the age inappropriate game resulting in more children wanting to follow suit.

Free Platforms

In order for a game to be released on popular platforms, such as PlayStation and Xbox, game developers must pay for a PEGI rating. However, smaller development teams are sometimes reluctant to pay these fees and games are often released on other platforms, such as Steam, without any age restrictions.

Spot the Signs

Being vague

Be aware of children being vague around the content of what they want to play. If they are unwilling to supply you with information about what the game is about, this can be an indicator that you wouldn't allow them to purchase it if you knew.

Unofficial sites

There are plenty of indie games that can be bought using online stores that don't necessarily have age restrictions. If you notice your child using sites such as GOG or itch.io rather than official channels such as the Google Play Store, they might be accessing games that aren't officially rated but still aren't age appropriate.

Unfamiliar terminology

Your child might start using phrases or terminology that is new to them or mimicking actions that they have learnt from a game without realising their inappropriateness.

Wanting to be secluded

Be aware if suddenly your child wants the move the device that they play their games on into a more secluded area of the house away from adults. It is a good idea for your child to play online games in shared area where you can see the screen.

Be aware of spending

Setting up accounts with online stores require bank account details. Keeping an eye on your bank balance means that you will be able to tell if there has been a new purchase and can provide you with an opportunity to ask about what new game they've purchased.

Safety Tips

Do your research

If you've noticed a new game that your child has downloaded then use quality resources to make sure that your knowledge is up to date. Online websites, such as National Online Safety, can provide you with the information you need.

Review parental controls

Review your parental controls on the stores where you buy games from. Most sites allow parents to set passwords to block games with certain age restrictions from being downloaded.

Encourage open dialogue

Encourage open dialogue with your child. You don't want to be in position where they won't talk to you if something has made them feel uncomfortable in a game because they are worried they will get in trouble for playing the game in the first place.

Discuss ratings

Talk to your child about why the game has been awarded a certain label. Debate the positives and negatives of playing a game and decide on some ground rules together.

Our Expert

Heather Cardwell

Heather Cardwell is a practising Online Safety Lead and senior school leader who is passionate about safeguarding online and educating children around online risks. She has over 10+ years as a Computing Lead and has successfully developed and implemented a whole school approach to online safety in schools, delivering online safety training to both school staff and parents and helping to roll-out a bespoke online safety policy across her local network of education settings.

Looking After Your

WELLBEING ONLINE

We all know that taking care of our minds and bodies is essential to keep us feeling happy and healthy. The thing is, we spend so much of our time online these days that it's also important that we remember to look after ourselves in the digital world, too. Our poster has got some simple but useful tips for supporting your wellbeing while you're gaming, on social media or just using the internet.

What Parents & Educators Need to Know about GROUP CHATS

On messaging apps, social media and online games, group chats are among the most popular ways that young people engage with their peers online. Involving three or more individuals, these groups allow users to send messages, images and videos to everyone in one place. While they can be great for connecting with others, there are several risks posed by these tools.

WHAT ARE THE RISKS?

BULLYING

Teens are often trying to find their place in their social group. Unfortunately, group chats can sometimes lend themselves to unkind comments being shared freely, putting people down to make their peers laugh – often creating a vicious circle that encourages others to join in. Being bullied so publicly – in front of friends and acquaintances – can also amplify the hurt, embarrassment and anxiety that the victim feels.

EXCLUSION AND ISOLATION

This common issue with group chats can happen in several ways: for instance, starting a new group, but deliberately excluding a certain child. Likewise, the chat may take place on an app which one person doesn't have access to, meaning they can't be involved. A child can also feel isolated when a group chat is used to discuss events that exclude them – for example, sharing photos from a day out that they didn't attend.

INAPPROPRIATE CONTENT

Some discussions in group chats may include inappropriate words, swearing and unsuitable images or videos. These could be viewed by a child if they are part of that group, whether they actively engage in it or not. Some apps have features that cause messages to disappear after they're viewed, so children may be unable to report something they've seen, as it can only be viewed once or for a short time.

SHARING GROUP CONTENT

Group chats can feel more private and protected, allowing children to share inside jokes and video calls with a smaller group of friends. It's important to remember that while the chat's content is private between those in the group, individual users can easily share material with others outside of the group, or screenshot what's been posted. The risk of something a child intended as private becoming public is higher if there are strangers in the chat.

UNKNOWN MEMBERS

Within larger group chats, it's more likely for children to communicate with people they don't know. These strangers may be friends of the host, but not necessarily friendly towards everyone present. It's wise for young people to avoid sharing personal details and remember that they have no control over what others do with the material they send into the chat.

NOTIFICATIONS AND FOMO

A drawback of large group chats is the sheer number of notifications they tend to generate. Every time someone sends a message, each member's device will be 'pinged' with an alert. This could result in hundreds of notifications a day. This is often highly distracting, and young people's fear of missing out (FOMO) can cause increased screen time as they try to keep up with the conversation.

Advice for Parents & Carers

CONSIDER OTHERS' FEELINGS

Group chats can become an arena for young people to compete for social status. This could cause them to do or say things on impulse which could upset others. Help children consider how people might feel if they behave in this way. If the child *does* upset someone, encourage them to reach out, show empathy and apologise for their mistake.

GIVE SUPPORT, NOT JUDGEMENT

Group chats are an excellent way for children to connect and feel like they belong. However, remind them that they can confide in you if they feel bullied or excluded, instead of responding to the person who's upset them. Validate their feelings and empower them by discussing how they'd like to handle the situation. You can also encourage children to speak up if they witness others being picked on.

BLOCK, REPORT AND LEAVE

If a child is in a chat where inappropriate content is being shared, advise them to block whoever sent the material, report that person to the host app or platform and exit the group. If any of this content could put a minor at risk, contact the police. Emphasise that it's OK for children to simply leave any group chat that makes them feel uncomfortable.

PRACTISE SAFE SHARING

In any online communication, it's vital for young people to be aware of what they're sharing and who might potentially see it. Ensure children understand the importance of not revealing identifiable details like their address, their school, or photos that they wouldn't like to be seen widely. Remind them that once something is shared in a group, they can't be certain where it might end up and how it might be used.

AVOID INVITING STRANGERS

Sadly, many individuals online hide their identity to gain a child's trust and serve their own ends – for example, to gather information on them, to exchange inappropriate content or to coax them into doing things they aren't comfortable with. Ensure the child understands why they shouldn't add people they don't know to a group chat – and why they should never accept a group chat invitation from a stranger.

SILENCE NOTIFICATIONS

Having a device bombarded with notifications from a group chat can be an irritating distraction – especially if it's happening late in the evening. Explain to children that they can still be part of the group chat while disabling notifications – and that it would be healthier for them to do so, avoiding a situation where they could feel pressured to respond.

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.

#WakeUpWednesday® The National College®

Sources: https://www.thinkuknow.co.uk/11_18/lets-talk-about/socialising-online/group-chats/ | https://www.nspcc.org.uk/keeping-children-safe/online-safety/social-media/chat-apps/

What Parents & Educators Need to Know about YOUTUBE

Almost anyone with an internet connection knows YouTube. The Google-owned site lets anyone upload videos to be shared around the world, and as a result, it's an incredible resource with instant free access to material covering every conceivable topic. But with over 500 hours of video uploaded every minute, not all of it will be appropriate for young eyes.

WHAT ARE THE RISKS?

INAPPROPRIATE CONTENT

YouTube is free and can be accessed via numerous devices, even without creating a YouTube account. Some content is flagged as 'age-restricted' (requiring the user to be logged into an account with a verified age of 18), but children can still view some mildly inappropriate content. This can include profanity and violence, which some young users may find upsetting.

CONNECT WITH STRANGERS

YouTube recommends videos related to what the user has previously watched on their account, aiming to provide content that will interest them. This is intended to be helpful but it can also lead to binge-watching and screen addiction – especially if 'auto-play' is active. Users without an account are shown popular videos from the last 24 hours, which might not always be suitable for children.

RADICALISATION

YouTube's algorithm tends to promote content that's getting the most traffic – a lot of which can be quite extreme. This can be fine for harmless topics, but YouTube isn't regulated like television, and that means that conspiracy theories, fake news and hateful ideologies can occasionally surface to warp impressionable minds all too easily. Remember – the more they watch, the more they'll be recommended.

CONNECTING WITH STRANGERS

YouTube is a social media platform which allows people to interact with other (usually unknown) users. Account holders can leave comments on any video they have access to, as well as message other users directly. Connecting with strangers online can potentially lead to children being exposed to adult language, cyberbullying and – in the worst cases – online predators. If a child is creating content themselves, this can increase the likelihood of them becoming a target.

TRENDS AND CHALLENGES

YouTube is teeming with trends and challenges, some of which are fun to watch and join in with. Children often find these immensely entertaining and might want to try them out. Most challenges tend to be safe, but many others may cause physical or emotional harm children who watch or copy them. The painful 'salt and ice challenge' – where people use these two ingredients to burn their skin – is just one of many examples.

SNEAKY SCAMMERS

The comments sections of popular content creators regularly have scammers posing as that influencer, attempting to lure users into clicking on their phishing links. Scammers impersonate YouTubers by adopting their names and profile images, and often offer cash gifts or 'get rich quick' schemes. Children may not realise that these users aren't who they claim to be.

Advice for Parents & Educators

APPLY RESTRICTED MODE

18 CENSORED

For older children, Restricted Mode is an optional setting that prevents YouTube from showing inappropriate material (such as drug and alcohol abuse, graphic violence, and sexual content) to underage viewers. To prevent children from chancing across age-inappropriate content on the platform, we would recommend enabling Restricted Mode on each device that they use to access YouTube. It's worth also turning the auto-play feature off, to prevent YouTube's algorithm automatically recommending something inappropriate.

TRY GOOGLE FAMILY

Creating a Google Family account allows parents and carers to monitor what their child is watching, uploading, and sharing with other users. It will also display their recently watched videos, searches, and recommended videos. In general, a Google Family account gives a parent or carer oversight of how their child uses sites like YouTube and helps to ensure that they are only accessing appropriate content.

MONITOR ENGAGEMENT

YouTube is the online viewing platform of choice for billions of people, many of them under 18. Younger children will watch different content to older ones, of course. You may want to keep an eye on how children interact with this material – and, if applicable, with content creators – to understand what they're interested in. Remember that creators often share content outside of YouTube, so don't ignore their web presence elsewhere!

CONSIDER YOUTUBE KIDS

It's possible to sidestep most inappropriate content completely via Google's own YouTube Kids app for Android handsets and iPhone. This lets you filter content by "preschool" (4 and under), "younger" (ages 5 to 8) and "older" (ages 9 to 12). This isn't a perfect substitute for personal supervision, as the app's filtering system is automated, and Google can't manually review all videos.

CHECK PRIVACY SETTINGS

YouTube gives users the option of uploading videos as 'private' or 'unlisted' – so they could be shared exclusively with family and friends, for example. Comments on videos can also be disabled and channels that a child is subscribed to can be hidden. If the child is only uploading videos set as 'private', they are far less likely to receive direct messages from strangers.

LIMIT SPENDING

Although YouTube is free, it does offer some in-app purchases. For example, users can rent and buy TV shows and movies to watch. If you'd like to avoid children purchasing content online, limit their access to online payment methods. Many parents have discovered the hard way that a child happily consuming a paid-for series quickly leads to an unexpected bill!

Meet Our Expert

Alan Martin is an experienced technology journalist who has written for the likes of Wired, TechRadar, Tom's Guide, The Evening Standard and The New Statesman.

#WakeUpWednesday®

The National College®