# E-SAFETY UPDATE



#### **HALF TERMLY UPDATE**

Welcome to our latest update! Lionheart Educational Trust is now sending out an e-safety update every half term, prior to the school holidays, in order to support parents and students. Due to the nature of widespread internet use at the moment, you will find this is a bumper edition this half-term, containing advice and support from a wider range of sources.

This update will feature resources by the National Online Safety organisation.

#### A FREE ONLINE SAFETY GUIDE ON CYBER RESILIENCE

In the last couple of decades, the volume of online traffic has increased exponentially - but, by and large, people's awareness of the accompanying risks hasn't grown along with it. To illustrate the scale of the issue, consider this: a report by the Internet Crime Complaint Centre found that, in the US during 2020, there was a successful cyber-attack every second. Yes: every second.

Criminals continue to find new and devious ways to attempt to hijack our online transactions and harvest our private information. To them, the smart devices that many of us now use as standard at home are simply a convenient back door into our lives - and our networks. Check out our #WakeUpWednesday guide for advice on beefing up your household's cyber resilience. In the guide you'll find tips on a number of potential risks such as how to use a password manager, how to back up your data and how to check for breaches.

#### A FREE ONLINE SAFETY GUIDE ON DIGITAL LIVES

Most parents frequently chat with their child about how things are going at school or what's happening in their friendship groups - but those discussions often doesn't extend to youngsters' online activities. In fact, National Online Safety conducted a recent survey which found that only slightly more than half (54%) of parents regularly talk to their children about staying safe online.

It can be an awkward topic to broach and, of course, it needs not to feel intrusive. However, just checking in with your child about their digital life can get them thinking about online safety and alert you to any issues they might be having. In support of Safer Internet Day 2023, our #WakeUpWednesday guide has some useful tips on potential ways to start those conversations.

In the guide you'll find a number of useful tips such as being as honest as possible, discussing how misleading the online world can be and creating a 'family agreement'.

#### A FREE ONLINE SAFETY GUIDE ON TWITTER

Twitter is a social media network which allows users to post short messages ('tweets') of up to 280 characters. Tweets can consist of text, photos, videos, audio, links, polls and GIFs - often linked by hashtags if they share a common theme or message. Hashtags receiving high levels of interest are said to be 'trending'. Twitter users can engage with other people's posts by liking, retweeting (sharing) or tweeting back (commenting on). Since the entrepreneur Elon Musk acquired Twitter in 2022 for \$44 billion, the platform has undergone several major changes.

#### A FREE ONLINE SAFETY GUIDE ON WORLD OF WARCRAFT

World of Warcraft originally launched way back in 2004, and since then the game has blossomed into a major entertainment property. It's spawned spin-off novels, merchandise and even a Hollywood movie adaptation ... but why are we still talking about it in 2023? World of Warcraft's most recent iteration, Dragonflight, launched last November and marks the game's ninth major expansion. This latest addition has attracted a whole host of lapsed players back to the game - as well as newcomers jumping into the realm of Azeroth for the first time.

In the quide, you'll find tips on a number of potential risks such as the potential for online addiction, in-game purchases and simulated violence.

#### A FREE ONLINE SAFETY GUIDE ON 10 WAYS GAMING CAN SUPPORT POSITIVE OUTCOMES

Gaming, of course, is phenomenally popular with children and young people. In 2021, for instance, more than three-quarters of teenagers played online games, with almost 70% of primary school aged children doing likewise. If enjoyed in moderation and supported by a healthy routine (staying hydrated, good sleep habits, taking breaks and so on), gaming can actually benefit a person's mental health. As long as we stay alert for potential risks, games can be much more than what we see on the surface: they can be a way to socialise, an avenue for creativity and a route to solving problems. Our top ten tips outline how gaming online can sometimes work to your child's advantage.

In the guide you'll find a number of potential benefits including a sense of achievement, learning about teamwork and encouraging creativity.



## 12 Top Tips for DING CYBER

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.



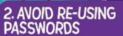
## WHAT IS 'CYBER RESILIENCE?'

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.



## 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. OSCAR123



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.

0

#### 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. LostPass, Dashlane, IPassword 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.

### 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.

## 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.

### 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.

## 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.

### 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.

## 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.

## 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 Sat. With a particular interest in digital citizenship and cyber security, he believes it is essential that adults and children alike become more aware.







National Safety #WakeUpWednesday

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



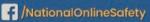
www.nationalonlinesafety.com



@natonlinesafety

RESTLIENCE

MAN





(O) @nationalonlinesafety

## Tips for Encouraging Open Discussions about

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

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

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

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

OW SHOW NG

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.

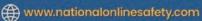
Involving your whole household in coming up with a family agreement about device use can be immensely beneficial. You could discuss when (and for how long) it's OK to use phones, tablets, consoles and so on at home; what parental controls are for and why they're important; and why it's good to talk to 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



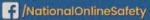


**National** #WakeUpWednesday





@natonlinesafety





## What Parents & Carers Need to Know about

WHAT ARE THE RISKS? Twitter is a social media network which allows users to post short messages (itwests) of up to 280 characters.

Tweets can consist of text, photosyvideos, audio, links, polls and GIFs = often linked by hash tags liftle yehre a common theme or message. Hash tags receiving high levels of interest are said to be 4 trending?

Twitter users can engage with other people's posts by liking, retweeting (sharing) or tweeting back (commenting on). Since the entrepreneur Flon Musk acquired Twitter In ectober 2022 for SAU billion, be bas implemented several perfect by passage to the class and the said of the control of the con \$44 billion, he has implemented several major changes to the platform.



## INTERACTION WITH STRANGERS

### PAID-FOR VERIFICATION

## HIJACKED HASHTAGS

CENSORED

## Advice for Parents & Carers

#### SET ACCOUNTS TO PRIVATE

#### EXPLORE THE NEW SETTINGS

#### **ENGAGE SAFETY MODE**

## Meet Our Expert



National Online #WakeUpWednesday



www.nationalonlinesafety.com



f /NationalOnlineSafety



(O) @nationalonlinesafety

## What Parents & Carers Need to Know about

WHAT ARE THE RISKS? World of Warcraft originally launched way back in 2004, and since then the game has blossomed into a major entertainment property. It's spawned spin-off novels, merchandise and even a Hollywood movie adaptation ... but why are we still talking about it in 2023? World of Warcraft's most recent iteration, Dragonflight, launched last November and marks the game's ninth major expansion.

This latest addition has attracted a whole host of lapsed players back to the game—as well as newcomers jumping into the realm of Azeroth for the first time.

## ALWAYS ONLINE

World of Warcraft is an MMORPG, which stands for Massively Multiplayer Online Role-Playing Game. Players create a character and head off on mythical quests to earn rewards and become more powerful. The game's environment is absolutely vast, and it can only be played online on PC or Mac – so there's a high probability of young Warcraft fans wanting to monopolise the family computer.

### REGULAR EXPANSIONS

is common with many MMORPGs As is common with many MMORPOs, World of Warcraft's developers, Blizzard, release regular expansions for the game (usually every 18 months to two years). So although there's still plenty of content for young players to experience right now, there will almost inevitably be a requirement to continue buying future expansion packs, which tend to cost around £50.

## IN-GAME PURCHASES AND SUBSCRIPTIONS

ust like its genre contemporary nal Fantasy XIV, World of Warcraft squires a monthly subscription fee to lay. It's currently £9.99 per month although you can get it cheaper by igning up to a longer subscription), here are also many items which can e purchased from the in-game store nat don't affect gameplay, but istead offer cosmetic alterations to a layer's character.

Because World of Warcraft is played exclusively on PCs and Macs, it's easy for users to type out text messages if they aren't comfortable using voice chat. If you'll forgive the pun, that's a double-edge sword because – although there's less chance of them being harassed verbally – it puts young players at increased risk of being trolled or receiving spam through the in-game messaging function.

### SIMULATED VIOLENCE

The fact that World of Warcraft is almost 20 years old means that even its most violent battles look slightly cartoonish compared with the level of authenticity in many more modern games. The exception tends to be Warcraft's in-game cutscenes: animated sections which move the plot onto the next stage. These offer more realistic visuals, but they still aren't overly gory or scary.

## POTENTIAL FOR ADDICTION

## Advice for Parents & Carers

#### SIGN UP FOR THE FREE TRIAL

### REMEMBER THE AGE RATING

### adventure together

## Meet Our Expert







National Safety

#WakeUpWednesday

ource:https://www.theguardian.co m/technology/2011/aug/29/world-of-warcraft-video-game-addict | https://worldofwarcraft.com/en-us/start



www.nationalonlinesafety.com







## 10 WAYS GAMING CAN SUPPORT POSITIVE OUTCOMES

## in Children and Young People

Gaming, of course, is phenomenally popular with children and young people. In 2021, for instance, more than three-quarters of teenagers played online games, with almost 70% of primary school aged children doing likewise. If enjoyed in moderation and supported by a healthy routine (staying hydrated, good sleep habits, taking breaks and so on), gaming can actually benefit a person's mental health. As long as we stay alert for potential risks, games can be much more than what we see on the surface: they can be a way to socialise, an avenue for creativity and a route to solving problems. Check out our top ten tips on how gaming online can sometimes work to your child's advantage ...

### ACHIEVEMENT & PRIDE

#### SOCIAL SALVATION

## A DIGITAL COMFORT

Daniel Lipscombe is a writer who specialises in technology, video gaming, virtual reality and Web3. Author of 15 guidebooks for children on games such as Fortnite, Apex Legends, Valorant Roblox and Minecraft, his work has also been published in the





National Online Safety #WakeUpWednesday

Source/https://www.ofcom.orgiuty/\_\_data/assets/pdf\_file/0024/234809/childrens-media-use-and-attitudes-report-2022.pdf



@natonlinesafety

