April 2023

E-SAFETY UPDATE

LIONHEART EDUCATIONAL TRUST

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 ARTIFICIAL INTELLIGENCE SOLUTIONS

Artificial intelligence is increasingly becoming a part of modern life and, for all intents and purposes, isn't something we can shy away from. The explosion of ChatGPT, for instance, has brought this kind of technology into a more purposeful context, with millions now using the language model to help solve problems, write computer code or even complete their homework.

So how do artificial intelligence solutions work exactly? What kind of risks do they bring? Will they eventually negate the need for certain job roles, particularly in the creative industries? This guide explains what AI solutions are and suggests ways parents and carers can support children to use the technology with an open mind. In the guide you'll find tips on a number of potential risks such as inaccurate information, reinforcing stereotypes and what impact the technology might have on children's creativity and problem-solving skills.

A FREE ONLINE SAFETY GUIDE ON NOT GONNA LIE (NGL)

NGL is another of those 'bolt-on' apps which is designed to work alongside a major social media network. In this instance, the 'host' platforms are Instagram and Twitter – with NGL (meaning, as you may have surmised, 'Not Gonna Lie') inviting a user's friends and followers to ask them questions anonymously. An intriguing novelty, perhaps – but also not without risk.

Human nature being what it is, some people take the smokescreen of online anonymity as an excuse to behave in ways that they certainly wouldn't if their identity were visible. The idea of exposing young social media users to anonymous messages is one which understandably concerns many parents: this guide brings you the facts about NGL. This free online safety guide looks at NGL – an anonymous messaging app.

A FREE ONLINE SAFETY GUIDE ON SAFE AND HEALTHY ONLINE HABITS

Every year, Comic Relief goes all out to help people, both in the UK and internationally, who are going through a tough time. In our area of specialism, we at National Online Safety are acutely aware that – for children and young people in particular – many of those difficult moments increasingly originate from and unfold in the digital world.

From inappropriate content to the toxic behaviour of others, online harms can do long-lasting damage. That's why we're passionate about helping this new generation to build their digital resilience – equipping them to deal with digital dangers. This guide has a selection of tips for encouraging safe and healthy online habits.

A FREE ONLINE SAFETY GUIDE ON STRONGER PASSWORDS

According to a Google survey, more than half of us (52%, to be exact) routinely re-use the same passwords, with around one in ten employing a single password across all of their online accounts. What that means, of course, is that any hacker successfully cracking our password would find themselves with access to not simply one of our online accounts, but several (at least).

That, along with the fact that many people's favoured passwords aren't exactly impenetrable, makes it easier to see why some sources put the number of online accounts being broken into at around 100 per second. Yes, you read that right: 100 per second. To help give you some extra peace of mind about your digital data, this guide has some tips on setting more secure passwords.

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

What Parents & Carers Need to Know about ARTIFICIAL INTELLIGENCE (AI) SOLUTIONS

AI solutions are becoming increasingly popular. Trained on vast datasets of text (such as books, articles and websites) in order to learn patterns and relationships, AI solutions can generate text, images, audio, video, code or synthetic data, and can be used for things such as crafting poems or books, creating digital imagery or delivering video content. Recently there's been significant discussion in relation to the benefits and risks of AI solutions, with many undecided on whether it will be a force for good or potentially reduce the need for some job roles.

WHAT ARE THE RISKS?

ROOM FOR INACCURACY

AI solutions, such as language models, generate their responses purely based on the data they've been trained on, which often comes from sources on the internet. Whilst questions will often illicit relevant responses, if some of the information they've been 'fed' is incorrect, it follows that the answers too may contain factual errors or inaccuracies.

REINFORCING BIAS

AI solutions, such as those generating content or images, can perpetuate existing biases present in the data they were trained, whether through the algorithms written by humans or the content taken from the web. This could easily lead to biased responses and potentially reinforce existing stereotypes, such as those around gender, race or disability.

IRRELEVANT INFORMATION

AI solutions don't have the ability to understand the context or meaning behind a question or a user request. Although highly advanced, the AI relies entirely on the data it's been exposed to and is devoid of independent thought or reasoning, which could lead to irrelevant or even nonsensical responses to queries.

LACK OF ACCOUNTABILITY

Fundamentally, AI solutions are machines or technology programmes that don't have the ability to take responsibility for the responses they generate. This could lead to confusion or misunderstandings in certain cases if the answers are taken as given. For instance, image-generative AIs can lead to output clearly derived from other peoples' content but without any attribution to the original source artist's work.

STIFLING CREATIVITY

One of the potential risks of children and young people continually using AI solutions for things (such as their homework) is that eventually, they might become reliant on it. In the long term, this could potentially impact their development and hamper their ability to think creatively or solve problems independently without the aid of an AI tool.

Advice for Parents & Carers

CREATE A SAFE ENVIRONMENT

If possible, try to be around when your child uses any type of AI solution and employ content filters to try and reduce the chance of profanity or age-inappropriate subjects appearing in responses. As with any kind of technology, it's important to ensure that children are using AI solutions responsibly and to be there to enable opportunities to discuss their use as part of a safe environment.

PROMOTE CRITICAL THINKING

Explain to your child that AI solutions can be used as one of many tools to help them research and learn, but that they shouldn't simply accept the responses they receive as the truth. Encourage them to question, verify and think critically about the information they get back – all of which apply equally to any website or platform they use.

DISCUSS BIAS

Talk to your child about the potential biases that may be present in the data that AI solutions are trained on, and how these viewpoints might find their way into the responses that AI generates. Again, with many things children might read online, it's healthy for them to consider whether the information is factual and presented fairly.

ENCOURAGE HUMAN INTERACTION

Not only should children supplement any use of software like AI with additional resources such as books and reputable internet sites, but they also should remember what they can learn from interaction with other people. Discussing things with teachers, relatives and friends isn't just an important and often invaluable aspect of learning – it's an essential part of life, too.

CHECK SCHOOL RULES

Make yourself aware of any rules or guidance your child's school might have about the use of AI solutions. Most software is still extremely new, so many schools may not yet have a policy, however, it's important to make sure your child is aware of how to use it appropriately and will be using it for the right reasons.

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: https://openai.com/blog/chatgpt/ | https://generativeai.net/ | https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-generative-ai

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 15.02.2023

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

What Parents & Carers Need to Know about NGL

AGE RESTRICTION 13+

NGL (which stands for 'Not Gonna Lie') is an app through which users share a link to their Instagram story or Twitter account, inviting their followers to give anonymous feedback. The app includes some prewritten questions (such as 'if you could change anything about me, what would it be?'), plus the option to ask followers to simply 'send me anonymous messages'. All replies go into the user's NGL inbox, with the sender remaining anonymous – although subscribers to the app can receive hints about who each message was from.

WHAT ARE THE RISKS?

ANONYMITY AND OVERSHARING

Anonymous messaging gives rise to the 'online disinhibition effect', which causes users to feel detached from their words and actions in the digital world. This can make young people in particular (as they tend to act more impulsively online) far more likely to disclose personal information on the internet, as well as making ill-advised confessions or revealing their fears and insecurities.

PROTECTION FOR BULLIES

Having their identity hidden makes bullies feel safe from repercussions, so anonymous chat sites are a major avenue for cyberbullying. NGL claims to use AI to filter out insulting terms, but our expert sent a range of such phrases (starting with 'cow' and 'ugly', and becoming progressively more offensive) to a 'dummy' account. All of these trial messages were delivered to the recipient's inbox.

COSTLY SUBSCRIPTIONS

NGL offers a subscription where – for a weekly fee – users can unlock hints about who's been messaging them, including the sender's approximate location and which device they used. Young people will naturally be extremely curious about who sent which message (especially if they have a lot of Instagram or Twitter followers) and may be unable to resist spending money to find out.

INFLATED ENGAGEMENT

1K

In June 2022, NGL had to revise its terms of service: informing users if a message was sent by the app's developers as opposed to genuine followers. It emerged that, previously, NGL's makers had attempted to boost engagement with the app (as well as enticing users to pay for subscriptions) by sending fake anonymous messages from bots. This update was rolled out very quietly by the team.

QUESTIONABLE SUPPORT

NGL *does* have a 'report this message' button for users to flag upsetting content. After sending a message, however, an automated reply arrives stating "... NGL is 100% anonymous and we have no way of knowing the identity of the user and would not be able to find out, even if we tried." This did not fill our expert with confidence that the app can address bad behaviour adequately.

ACCIDENTALLY GOING VIRAL

The messages on NGL itself are anonymous, but users can share these messages via their Instagram story or Twitter feed – enabling all their followers (or anyone, if their accounts are set to 'public') to see them. If a young person has disclosed something embarrassing or identifiable on NGL without realising, this information has the potential to be re-shared very quickly to a far wider audience.

Advice for Parents & Carers

DEALING WITH NEGATIVITY

Blocking another user on NGL will prevent them sending anonymous messages to your child in the short term – although a determined abuser could get around that obstacle simply by setting up a new Instagram account. If your child continually receives negative messages that upset them, it might be worth encouraging them to consider whether they really need to use the app at all.

BLOCK IN-APP PURCHASES

To avoid your child running up an eye-watering bill through an NGL subscription (or indeed any kind of costly in-app purchases), go into the settings on whatever devices they use to go online and either disable the ability to make purchases or protect that function with a password. If those options aren't available, it's prudent to ensure there aren't any payment methods linked to their account.

EXPLAIN ANONYMOUS APPS

We understand that a conversation with your child about the risks of anonymous messaging may seem difficult to initiate (especially if you aren't that comfortable with using social media yourself). It is vital, however, that young people understand that, for some people, having their identity obscured online can make them feel more powerful and less accountable for their actions.

THINK BEFORE SENDING

Regardless of whether a messaging app is anonymous or not, it's a good idea to regularly talk to your child about how it's wise to think through what they're sharing before they post it. Emphasise that nothing is truly private once it's online. If the post is something your child might hesitate to say to someone face to face, then it's probably not the sort of thing they should be writing online either.

Meet Our Expert

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

NOS National Online Safety®
#WakeUpWednesday

Source: https://ngl.link/#what-s_ngl

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 01.03.2023

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

Top Tips for Adopting SAFE & HEALTHY ONLINE HABITS

Everyone has so much going on in their lives, and that includes children: from exams and deadlines to anxiety and mental health struggles. It's quite easy to send memes, make jokes and vent online about the things that irritate us, but when was the last time you – or your child – took a moment to share something kind or positive instead? In fact, when did you last stop and think about your family's online activities? To help keep them safe and teach them healthy online habits, we need to develop our children's digital resilience. There are lots of ways that children can become more digitally resilient, and we've pulled together some popular strategies here ...

WHAT IS DIGITAL RESILIENCE?

Resilience doesn't mean being so tough that nothing gets to you, and it's not about "putting up with things" either. Instead, it's the ability to recover from setbacks. Everyone feels sad, worried, scared or upset at times: it's how we respond and adapt to those situations which is important. Digital resilience is about making choices that keep us safe and happy online, even when we're exposed to something negative or upsetting. Building your child's digital resilience will help reduce the impact of potential risks as they engage with and navigate around the online world.

MAKE POSITIVE LIFESTYLE CHOICES

- Make time for the people and things that make you happy.
- Monitor your screen time and stick to your limits.
- On social media, follow people that make you feel good about yourself – and unfollow the ones who don't.
- Spread some positivity: post good reviews, leave encouraging comments and share good news.

KEEP YOUR HEALTH IN MIND

- Try to factor in regular breaks offline and away from your screen – ideally, outdoors for some revitalising fresh air.
- Exercise is a brilliant stress-buster: even a walk around the block, a bike ride or a stroll to your local shop can really work wonders.
- Be strict with yourself about putting devices away in plenty of time before bed: they can interfere with a good night's sleep, which is essential for staying healthy.

REACH OUT FOR SUPPORT

- If you have a problem online, don't be afraid reach out to specialist people or organisations that could help.
- Follow people on socials who have the same values and morals as you.
- You could always talk to a friend, or a trusted adult like a teacher or family member for some advice.

PUT SAFETY FIRST

- If you see something online that upsets or worries you, tell a trusted adult about it as soon as possible.
- You could also report the content that's making you feel uncomfortable to the site or app that you saw it on, so they can look into it.
- Another option is to block the person or the account that's causing you a problem – or you could go one step further by totally deleting the app you were using.

GET THINGS CLEAR IN YOUR HEAD

- Ask yourself what kindness online actually looks like. Can you remember the last time someone was kind or supportive towards you online? What did they do?
- Think about how it makes you feel when someone sends you a positive or funny message online.
- What about the opposite: has someone ever been deliberately unkind to you online? What did they do and how did it make you feel?
- If someone's behaviour online is causing you stress, try to remind yourself of all the steps you can take if a person's being unkind online.

Meet Our Expert

Cayley Jorgensen is a registered counsellor with the Health Professions Council of South Africa, working in private practice to offer counselling to children, teenagers and young adults. She is the founder of Ingage Support, a mobile app focusing on mental health awareness with the goal of providing resources and solutions to schools worldwide.

NOS National Online Safety®

#WakeUpWednesday

@natonlinesafety /NationalOnlineSafety @nationalonlinesafety @national_online_safety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 15.03.2023

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

Ten top tips for STRONGER PASSWORDS

Passwords continue to be the most common way to prove our identity online. A combination of a username and a password known only to the user provides access to our online accounts and data – and hopefully keeps unauthorised individuals out. As a security measure, though, passwords are relatively weak. People are often predictable in how we choose our passwords, for example – making them less secure. With increasing volumes of usernames and passwords being leaked online, what can we do to keep our data more secure? Here are our top tips for stronger passwords.

BE UNPREDICTABLE

We often choose passwords which are easy to remember: featuring the name of our favourite sports team or favourite film, for instance. Those are predictable passwords. Cyber criminals will routinely try various combinations of passwords relating to sports teams, actors, musical artists and the like – and they often focus on these during major sporting events or around high-profile movie releases.

AVOID GETTING PERSONAL

Many of us use passwords relating to our family, such as children's names or favoured holiday destinations. The problem here is that we also typically post about our holidays and our family on social media – making that information potentially visible to cyber criminals and supplying them with clues which could help them in narrowing down possible passwords we might have set.

NEW PLATFORM, NEW PASSWORD

Where cyber criminals gain access to an online service through a data breach, they often use the data they've stolen to try and access the victim's other accounts. This is because the criminals know that, for convenience, people often use the same password across different services. When we reuse passwords, our security is only as strong as the weakest site where we've used it.

LONGER IS STRONGER

Our passwords are often stored by online services in an encrypted format, in case the service suffers a data breach. The strength of this encryption, however, is dependent on the length of the password you've selected. If your password is only a short one, cyber criminals are significantly more likely to be able to break the encryption and identify your password.

CHECK SOCIAL MEDIA VISIBILITY

Staying up to date with friends and relatives on social media is part of everyday life now. We need to ensure, though, that we limit who can see our posts via each platform's privacy settings. It's also wise to consider what we're posting and if it's *really* safe to share online. If we restrict what cyber criminals can see, we reduce the chance of them using that information to identify our passwords.

'DOUBLE LOCK' YOUR DATA

It's possible that cyber criminals may eventually discover your username and password. Enabling multi-factor authentication (MFA) on your accounts, however, reduces the chance of them obtaining access to your data, as they'd also require a code which is provided via an app, SMS message or email. MFA isn't infallible, but it *does* definitely provide extra protection and security.

DELETE UNUSED ACCOUNTS

Data breaches occur when cyber criminals gain access to an online service and all the data contained within it – including usernames and passwords. Whenever you stop using a service, it's wise to make sure that you delete your entire account and not just the actual app. If the service no longer has your data, there's zero risk of it being leaked should they suffer a data breach in the future.

TRY PASSWORD MANAGERS

Even though most of us have numerous online accounts to manage these days, it's advantageous to avoid password re-use. Specialist password management software (like Dashlane or OnePassword, among others) can help by storing a different password for every online service that you have an account with: the only one you or child will need to remember is the single master password.

GET CREATIVE

The British government's National Cyber Security Centre (NCSC) recommends the 'three random words' technique. This method helps you create a password which is unique, complex and long – yet which is memorable enough to stay in your mind ("FourBlueShoes", for example). The NCSC website, incidentally, also offers plenty of other useful information relating to personal cyber security.

STAY VIGILANT

The best way to protect your accounts and your data is to be vigilant and careful. If you receive an email or text message that's unusual or unexpected, treat it as suspicious until you're able to verify whether it's genuine and safe. Starting from a position of vigilance and caution will reduce the likelihood of you or your child being tricked by a malicious email, text or phone call.

Meet Our Expert

A Certified Information Systems Security Professional (CISSP), 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 we become more aware of the risks around technology, as well as the benefits.

National Online Safety®

#WakeUpWednesday

Source: https://www.ncsc.gov.uk/

@natonlinesafety /NationalOnlineSafety @nationalonlinesafety @national_online_safety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 22.03.2023