October 2024

E-SAFETY UPDATE

LIONHEART EDUCATIONAL TRUST

TERMLY UPDATE

Welcome to the Lionheart Educational Trust's termly E-safety update!

This is to support parents and students to stay safe online. This update will feature resources by the National Online Safety organisation and these can also be found on our school websites.

A FREE ONLINE GUIDE ON STRONGER PASSWORDS

As we settle into the new academic term, students will be logging into our IT systems using their login credentials given by the school. Students should regularly change their passwords and these need to be strong passwords for their accounts to remain secure.

Year 7 will be talking about strong passwords in their Computer Science lessons and why its important to regularly change them.

This guide provides some tips to discuss with your children about setting strong passwords for any online accounts they create.

A FREE ONLINE GUIDE ON THE USE OF AI

The use of AI solutions is becoming extremely popular in Education. This is an excellent tool to use when used properly. AI can be used on various datasets (such as digital books, articles and websites) to learn patterns within the datasets. AI solutions can generate text, images, audio, video and code.

It is important that students reference any use of AI in their work. AI should not replace the work students are expected to do; however, it can be used to help students develop better understanding of key learning principles within their subjects. Subject teachers will be able to provide further guidance on this to students based on the course requirements. This guide provides details of risks associated with the use of AI as well as how to use AI safely.

A FREE ONLINE GUIDE ON ONLINE CONTENT

The Internet is a great resource in education and has enabled students to access vast amounts of online content. This include access to Apps that students use which are include user-generated content. Due to the shear volume of content uploaded online, it is difficult to monitor and filter content that is age appropriate.

The two guides provide tips for parents on how to keep children safe online and includes questions to help start those important conversations.

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

HELLO MY NAME IS OSCAR

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

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.

NOS 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

www.nationalonlinesafety.com @natonlinesafety /NationalOnlineSafety @nationalonlinesafety

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 they need to hold an informed conversation about online safety with their children, should they feel it is needed. This guide focuses on one issue of many which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.

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

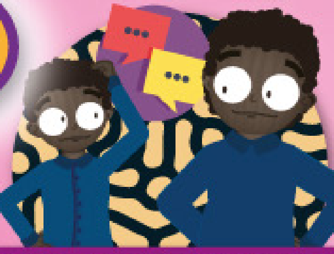
Ensure they know that there is support and advice available to them if they need it.

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.

NOS National Online Safety®

#WakeUpWednesday

www.nationalonlinesafety.com Twitter - @natonlinesafety Facebook - /NationalOnlineSafety Instagram - @NationalOnlineSafety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 16.09.2020

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

National Online Safety®

#WakeUpWednesday

Conversation starters for parents and carers: ONLINE CONTENT

Trying to start a conversation about online safety with children can be a daunting task. There are many reasons why children may not want to talk to adults about it. One might be that they don't think you'll understand or that you won't know how to help if they came to you with an online problem. It can also be hard to start a conversation about something that you might have limited knowledge about. However, with screen time increasing during the lockdown, it's important now more than ever, to be talking to children about what they are accessing online.

1 ASK THEIR MOTIVATION

Sometimes it's easy to assume we know why children choose certain games or apps. It can seem obvious, like the child interested in football will be enthusiastic about the new FIFA game. But sometimes it can be more subtle than that. It could be that it's an outlet for their creativity or it might be that they like the look of the main character. Learning their motivation and knowing why they like it can help advising them on how to use it safely and help you discuss the pros and cons.

2 CULTIVATE A BLAME FREE CULTURE

Children can often blame themselves if they come across something that scares them or makes them feel uncomfortable. There will be times when your child has gone against something that you have forbidden, however, most children do not intend to put themselves at risk. Therefore, it's important that your child is able to come to you with a problem and won't be blamed for it. Try to understand what happened and why and warn them of the dangers once more. Engaging in a 'told you so' dialogue or suggesting they are in trouble for not listening may deter them from reporting any future concerns.

3 SHARE PERSONAL EXPERIENCE

Starting a conversation by sharing something that you've seen or that has made you feel uncomfortable can be a great opener. Talking about your own feelings can help children realise that it isn't just them – adults can be affected too. You can then go into how you coped with it therefore indirectly giving children advice on how they can also cope in uncomfortable situations. You can also explain that the reason that you've chosen to talk to them about it is because talking helps. Children will hopefully be able to see the parallels in the experiences and mimic your behaviour in future.

4 TALK ABOUT THE NEWS

Asking children what their response is to news stories around online safety can be revealing. For example, there has been a recent survey conducted by the BBFC who are currently campaigning for the application of age ratings and content warnings on video sharing platforms. What do they think about this? Can they think of a time when this would have helped themselves or someone they know? Are they against the idea? If so, why? Could they be accessing something they shouldn't be?

5 ASK FOR ADVICE

It could be that you really do have a friend at work who is debating whether or not to let their child do something online, or it could be that you're bending the truth slightly, but hopefully the outcome would be the same. Don't be afraid to ask others for advice. Not only why they should let the child use it, but also what would they tell the child to be aware of. What are the risks? This will help you understand the risks yourself and what to look out for in future.

6 MAKE TIME TO LISTEN

When your child can't wait to tell you about their new game, always try and listen to what they say. We always have a lot on our minds, so it's easy for us to drift off onto other things which may be more important. However try to stay involved and ask them more details about aspects of the game/app. Children will appreciate your interest and the more questions you ask, the more you can find out. If you act uninterested, then they are less like to tell you about it again in the future.

7 ASK THEM TO BE THE TEACHER

Showing an interest in what children are accessing online is a great opportunity for you to learn something new as well. Children on the whole love sharing their experiences so by asking them to teach you how to use an app or play a game is not only a great way to bond, but you will also feel more empowered to talk about it. It is easy to shy away from conversations when the child perhaps knows more about the subject content than you do. This can help to turn this around.

8 USE SCHOOL MESSAGING

It might be that your child's school has sent out a message about the Childline number or to remind children to use the CEOP button to report content. Ask the children what they learned about these at school. When would they use the Childline number? When would they need to use the CEOP button? What does it look like? Asking the children why the school thought that the information was so important that they sent out a message about it reinforces what they learnt whilst at school.

9 ASK ABOUT THE RISKS

Many children may know what online risks are and will happily explain the potential dangers. Listen and try not to be overly shocked if they tell you something that disturbs you. This can then lead nicely into you asking the question about what steps they are taking to look after themselves or what help they could seek if something goes wrong. Sometimes it's just nice to know that your children know the dangers and have taken steps to help reduce the risk for themselves – this is the ultimate goal.

10 ASK ABOUT RESPONSIBILITIES

Try asking open ended questions about roles and responsibilities online. Who is in control of the internet? Who is looking after you whilst you are online? Who decides what is appropriate for children to see? This can reveal a lot about a child's perception about who is responsible for their online safety. If they believe that it is up to everyone else to keep them safe, then you know you need to have a conversation about how they can reduce their own risk.

Meet our expert

Heather Cardwell is a practising Online Safety Lead and senior school leader who is passionate about safeguarding children online and educating them 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.

11 ASK ABOUT SCHOOL ADVICE

Sometimes it's hard to know what to warn children about. If there is a new app or game that your child has come across recently, ask them what they think their teacher would say about it. What advice would school give them? What have they been told about trusting people online or about fake news? Finding this out would be a good way to hear what advice they were given at school and help you reiterate the same message. Quick reminders about what to do if something makes them feel uncomfortable or who their trusted adults are can make all the difference.

www.nationalonlinesafety.com Twitter - @natonlinesafety Facebook - /NationalOnlineSafety Instagram - @nationalonlinesafety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 24.06.2020