PADGATE ACADEMY

SAFEGUARDING NEWSLETTER

PADGATE ACADEMY

February 2023

Welcome to the second safeguarding newsletter of the year. February is a busy month, packed with exciting events such as Children's Mental Health Week, Safer Internet Day, and LGBT History Month. In this edition of the newsletter, you will find information on these topics which will hopefully prove helpful.

As always, we have included signposting to some key agencies, should you require their support.

Kind regards,

Ms Jones and the Keep Kids Safe team.

KEY NUMBERS

Anyone can contact the services below directly, regardless of whether you are a child, parent, carer or a member of staff. If you have a safeguarding concern, please ensure you pass it on: safeguarding is everyone's responsibility.

01925 443322 (Option one, followed by option one) **Warrington Multi-Agency Safeguarding Hub (MASH)** For urgent safeguarding concerns about a child	**01925 443322** (Option two) **Out of Office Emergency Duty Team** For urgent safeguarding concerns about a child outside of office hours	**0808 800 5000** **NSPCC** For adults who are worried about a child
0800 1111 **Childline** For children who are worried about their own safety or need some advice	**101** **Police Non-Emergency** For reporting any crimes or concerns	**999** **Emergency Services** For anyone in immediate danger (including if you are worried about the immediate risk to a child)

Upcoming Events

Safer Internet Day

We will soon be sending out an email regarding Safer Internet Day which is celebrated on 7th February. Our students will be participating in lots of activities in their IT lessons throughout the week, to keep the awareness going. On Tuesday, students will be discussing how to make connections safely online using resources provided by Place2Be as part of Children's Mental Health Week: thus, bringing the two events together nicely.

There are lots of links in the letter sent out by Mr Piggott (Trust IT Lead), which will hopefully provide some helpful guidance on various issues such as parental controls, safe technology and a guide to apps.

The NSPCC link is particularly useful, as it has an up-to-date list of the apps a lot of our children are currently using. For convenience, here is the link again: https://www.nspcc.org.uk/keeping-children-safe/online-safety/social-media/

The official Safer Internet Day website also provides a handy guide for parents on holding healthy conversations with children about life online (& lots more!): https://saferinternet.org.uk/safer-internet-day/safer-internet-day-2023/top-tips-for-parents-and-carers

At the end of this newsletter, you will find a guide with 12 top tips for cyber resilience in the home. In school, we are having a particular push on ensuring that all passwords are strong and secure.

Time to Talk Day & Wellbeing Drop-in

Thursday 2nd February is Time to Talk Day. The aim of this day is to get the nation talking and encourage discussions about our mental health. Talking about mental health is often difficult, but having that conversation can be powerful and life-changing.

To mark the occasion, the student mental health ambassadors are launching a weekly wellbeing drop-in every Thursday lunchtime for all students. This will be held in the library, and there will be different stations across the room to suit different needs. There will be a quiet reading corner, an activity station, and a space for students to gain peer support from the mental health ambassadors. Our ambassadors have come up with lots of ideas and there are plenty of exciting plans coming up. We are incredibly proud of these students and extremely grateful for the effort they continue to put in, to make this drop-in a success!

Children's Mental Health Week

Children's Mental Health Week is celebrated on 6th – 12th February this year and the theme is 'Let's Connect'.
In school, we are collapsing our usual tutor time program and replacing it with important activities based around mental health and connecting with others.

In KS3, they will first learn about why connection is so important and the link to mental health. They will then go on to learn about how to connect safely online, and be taught communication skills in order to effectively manage disagreement and difference in a healthy and productive way.
In KS4, they will also be taught the links between connection and mental health, before going on to explore healthy relationships, non-verbal communication, and effective communication.

Excitingly, all students in years 7-10 will be taking part in creative sessions led by Warrington Youth for Christ as part of 'The Champion Tour'. This hour-long session will explore the managing of stresses and overcoming the challenges of life in a creative and relevant way that is both motivating and inspiring using music as the medium and with a specialist mental health practitioner. All students are then able to watch them perform their music at a unique lunchtime gig!

Below are some services available to provide children with mental health support:
For children in crisis, you can call the Crisis Line on 0800 051 1508.

www.kooth.com
A free, anonymous instant messaging service for young people

www.youngminds.org.uk
The Young Minds website contains lots of resources, real life stories and signposts to support children with mental health difficulties

www.samaritans.org
The Samaritans are a charity who provide emotional support to anyone who needs it. You can call or email them to speak to someone.

LGBT+ History Month

Continuing the list of exciting events in February, we have LGBT+ History Month. This provides an excellent opportunity to explore the past and celebrate how far things have come when it comes to all things LGBT+.

In school, we will firstly be holding assemblies to all students looking at the impact of homophobic/transphobic language, before going on to have a second week of assemblies celebrating the amazing and rich history of the LGBT+ community.

We hope you have found this newsletter useful. For further safeguarding information, please visit the school website: https://padgateacademy.co.uk/safeguarding

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.

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

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: 25.01.2023

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.

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

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: 01.02.2023