

Safeguarding Newsletter



MARCHWOOD C OF E INFANT SCHOOL

AUTUMN 2023

Welcome to our latest edition of our Safeguarding Newsletter from Marchwood Infants' safeguarding team. This newsletter is designed to bring you the latest, relevant help and advice on issues we feel will be of importance to you. Previous editions can be found on our [website](#).

Safeguarding children is the action we take to promote the welfare of children and protect them from harm. Safeguarding is everyone's responsibility and anyone who comes into contact with children has a role to play.



Spotlight on: managing screen time

With the half term holiday upon us, we have included some helpful information about managing screen time to help parents and carers understand the risks and what you can do to keep your child safe.

Spending time online and on devices can be a positive thing. But, high levels of screen time can put your child more at risk of:

- Being bullied online
- Abuse and grooming (when someone builds a relationship with a child to exploit or abuse them)
- Seeing inappropriate content
- Not getting enough sleep and exercise

4 steps you can take to protect your child

Set parental controls on devices to: • Restrict access to in-app purchases and explicit or age related content • How long they can spend on the device <i>You'll probably need to set a password. Make sure it's different from the password used to access the device and your child doesn't know it.</i> Parental controls are usually located under 'Settings'.	Agree rules on screen time • Plan together and stick to it; e.g. media free times and zones • Avoid screens 1 hour before bed • Model the behaviour • Minimise snacking during screen time <i>Turn not using screens into a game, using apps like Forest, where not using devices is rewarded</i>
Talk to your child about staying safe online • Anyone can pretend to be a child online • Don't give away personal info (e.g. where they live or go to school) or share their location • Set their profiles to private • Be 'share aware' - once it's out there, there is no control over what's done with it.	Encourage off screen activities • See www.nhs.uk/change4life/activities for free ideas for activities and games • Try an app that's designed to get children active – see the examples at www.internetmatters.org/resources/apps-guide/apps-to-help-kids-get-active/ or use our Bursts app which rewards daily physical activity.

Don't feel confident starting a conversation with your child about what they're up to online? Read this advice from the NSPCC: <https://www.nspcc.org.uk/keeping-children-safe/online-safety/talking-child-online-safety/>

What to do if you're concerned about a child

If you are worried about a child's safety, please contact one of our designated safeguarding leads (DSLs).

MIS Safeguarding Team



Mrs Lucy Chambers
DSL



Mrs Fleur Fisher
Deputy DSL

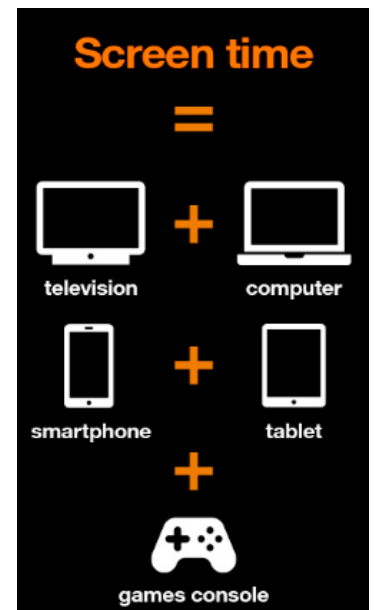
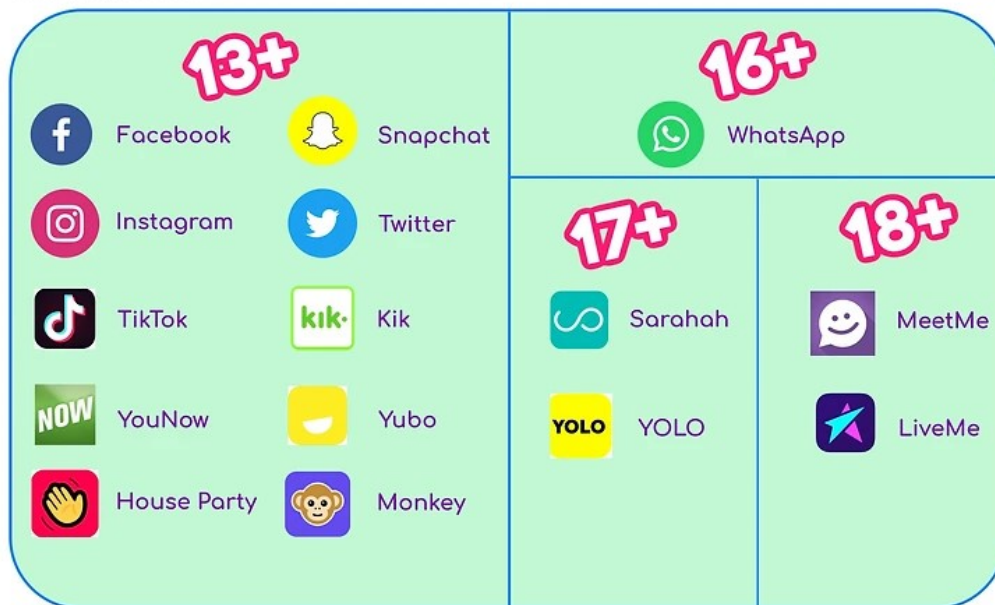


Mrs Marrianne Andrews
Deputy DSL



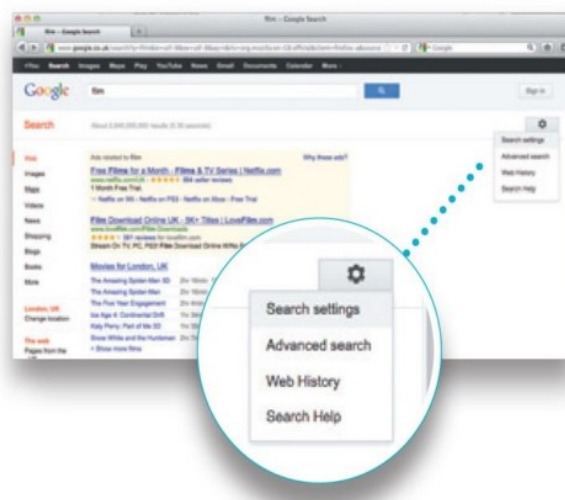
Mrs Claire Besant
Deputy DSL

APPS AND THEIR AGE RATINGS



Google SafeSearch

SafeSearch helps you to keep adult content out of search results by screening websites that contain sexually-explicit content and removing them from the search results.



Childnet—Online resources

Childnet has created a range of resources on important topics such as digital wellbeing. These are designed to help parents and carers offer support and guidance to navigate the internet safely and positively.

Key safeguarding information and documents can be found on our website:

[Safeguarding | Marchwood Church of England Infant School \(marchwood-inf.hants.sch.uk\)](https://marchwood-inf.hants.sch.uk)

Helping children and young people with MANAGING DEVICE STRESS AND ANXIETY

WHAT ARE THE RISKS?

The internet and advances in the capability of digital devices have afforded us arguably the fastest period of technological and social evolution in living memory: creating opportunities for us to interact with people anywhere in the world, 24 hours a day. It's also, however, blurred safety boundaries and added new stresses for young people, who are often less aware of the hidden hazards. With almost half of 10-15-year-olds experiencing bullying online and algorithms pushing content in front of our children every day, it's important to know how to address some of these challenges.

LIVING ONLINE

The internet is awash with sophisticated algorithms that learn from our online behaviour and try to predict our wants and needs. That's very helpful in some respects, but it can make the online world difficult for children and young people to negotiate. Content can be brought to them at any time – it may not always be appropriate, and children may not have the ability or the support to deal with it.

PUSHY NOTIFICATIONS

Content is also directed at us through notifications from our apps: letting us know we have a new message or social post to read, for example. While that's useful in some circumstances, it conditions us to keep going back online (and is designed to do so) and can be a near-constant demand on your child's attention. As such alerts become more common, are we experiencing an 'attack of the pings'?

BLURRED BOUNDARIES

There are now so many ways we can communicate online in real time (like instant messaging apps) or with a delay (such as on social media) that it's possible to be constantly in conversation. Young people often prefer quickfire exchanges of text – but using fewer words can cause distressing miscommunications through the lack of non-verbal cues like facial expressions or tone of voice.

DIGITAL DEPENDENCY

As devices allow access to immediate external help in challenging situations, it's a concern that children may not be developing the inner confidence to work things out for themselves. Likewise, group membership is hugely important to young people – both in digital and 'real' life – and being excluded from online conversations can cause damaging feelings of loneliness and isolation.

DISGUISED DISTRESS

Children often haven't yet developed the emotional resources to deal with many of the setbacks of everyday life, so identifying when it's specifically something online that's worried them can be tricky. A certain level of stress is a normal response to a problem: it spurs us into action to keep ourselves safe. If the stress is excessive, though, it can feel overwhelming and potentially lead to anxiety or depression.

ANTI-SOCIAL SOCIALS

Social media can bring people together in hugely positive ways. Sadly, it does also have a darker side, including 'flame war' arguments which can escalate quickly and have harmful consequences. With so many people looking on, 'group shaming' situations are also common – while there are continual opportunities for young people to compare themselves negatively with other social media users.

Advice for Parents & Carers

LEARN THE BASICS

It's impossible to keep up with every online change or every new app. The best option is to make yourself aware of the fundamentals of how the internet operates, so you can help your child to grasp how – and why – content reaches them. Devices and the digital world can be confusing, so learning to understand them better will give you the confidence to talk to your child about them.

TALK IT OUT

If a child mentions a comment that's been directed at them in a text chat or on social media, it may sound minor but can actually have a much bigger effect than we realise. In our evolved brains, any perceived threat can get internalised while our body reacts as if we were in physical danger – raising stress levels. It's always worth encouraging your child to get any concerns out in the open.

PUSH DISTRACTIONS AWAY

Notifications to our phones and tablets can be helpful, but they sometimes make one wonder who's really in charge: the person or the device? Checking our phone as soon as it goes off is an easy habit to fall into – especially for young people. Try switching off non-essential alerts on your devices and encourage your child to do the same: you should both feel less triggered and more in control.

LOOK FOR THE SIGNS

This is tricky – and may depend on the child's age – but any sudden change in behaviour is worth looking out for. If your child seems to be checking their phone or tablet more, doesn't want to be parted from them, or appears unusually secretive, anxious or withdrawn, it could be a sign that something is amiss in relation to their device – and, possibly, that they're in need of extra support.

KEEP CHECKING IN

Healthy emotional regulation balances three systems: threat, drive and grounding. Down the various rabbit holes of the internet, however, that balance can easily slip away – so it's important to help your child manage their emotions when they're online. Check in with them regularly when they're on their device, and remember that 'distraction' and 'relaxation' aren't always the same thing.

BE KIND: UNWIND

Be kind to yourselves as parents and carers. Remember that we're all in the same boat, trying to safely guide our children through this complex, fast-moving digital environment. Getting into the habit of having natural, relaxed conversations with your child about their online life (and yours) can level the playing field and make it far easier for them to open up to you about any concerns.

Meet Our Expert

Dr Carole Francis-Smith is an experienced counselling psychologist who specialises in promoting safe and ethical online communications. She consults with and offers bespoke training to businesses and organisations, supporting positive and effective online communications – often by considering some of the more hidden aspects of the various mediums.



**National
Online
Safety**

#WakeUpWednesday

Source: <https://www.childrenscommissioner.gov.uk/report/the-big-ask-big-answers/>
<https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/childrensonlinebehaviourinenglandandwales/yearendingmarch2020>



@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: 29.03.2023

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.

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.



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

CCTV
IN OPERATION

'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.

 **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: 22.03.2023