E-SAFETY NEWSLETTER

BALLIOL PRIMARY SCHOOL

December 2023

For more tips and information, please visit our school page: https://www.balliolschool.co.uk/e-safety/
Sign up here for a free weekly parent e-safety newsletter: https://www.internetmatters.org/about-us/newsletters/

Setting up gaming consoles this festive season

Are you planning on gifting a phone, games console or tablet this festive season?
Here is a tech guide for 2023: https://www.internetmatters.org/resources/tech-guide/
Did you know that they all come with free parental controls that help you to limit things like the time children spend playing, who they interact with and what additional purchases they can make? With Christmas just around the corner, we thought we'd provide a little reminder about setting up appropriate parental controls for any new phones, consoles or games your child may receive.

Games/consoles

First, check the PEGI rating of any new games to check that your child is old enough to be playing them. PEGI provides age classifications for video games and considers the age suitability of a game, not the level of difficulty. It is important to note that PEGI do not take into consideration user generated content within games (such as on Roblox) and the chat facilities within games. Visit PEGI here: https://pegi.info/

For any new consoles, it is important to set up appropriate controls such as restricting spending limits and managing who they can communicate with. Follow the links below to find out about Parental Controls for each device:

Nintendo:
https://www.nintendo.co.uk/Hardware/Nintendo-Switch-Parental-Controls/Nintendo-Switch-Parental-Controls-1183145.html

PS5:
https://www.playstation.com/en-gb/support/account/ps5-parental-controls-spending-limits/

Xbox:
https://www.xbox.com/en-GB/community/for-everyone/responsible-gaming

Other guides can be found here:
https://www.internetmatters.org/parental-controls/gaming-consoles/

Tablets/Smart phones

As well as setting up parental controls on the device itself, remember to check any apps your child would like on their device, is it suitable for their age and review all settings and privacy options for each one. For the devices, use the available settings to prevent purchases, restrict content viewed and adjust privacy settings. Follow the links below to find out more:

iPhones/iPads:
https://support.apple.com/en-gb/HT201304

Google Play:
https://support.google.com/googleplay/answer/1075738

Further information

Information, tips and advice on setting up parental controls:
https://www.nspcc.org.uk/keeping-children-safe/online-safety/parental-controls/

Little Digital Helps Toolkit

What is it?

Created with their partner Tesco Mobile, this is a one-stop shop for all the things you need to set controls and privacy settings on new and old devices that your children use, with plenty of advice on how to deal with online risks. Internet matters also made sure to include tips on how to make the most of their digital world, based on what they like to do. It only takes 8 minutes to fill in a few questions about your children's digital habits to receive a tailored toolkit, packed full of resources to keep them safe on connected devices.

Find out more here: https://www.internetmatters.org/little-digital-helps-toolkit/

Where can I find other age ratings?

It's important that we follow these to ensure that what our children are doing or seeing online is appropriate for their age.

• Films: The British Board of Film Classification (BBFC) rate films. This page includes a link to a 'Parents' Guide to Age Ratings': https://www.cbbfc.co.uk/resources/viewing-films-safely-online
• Video games: PEGI provides age classifications for video games. PEGI considers the age suitability of a game, not the level of difficulty.
• Apps: Check the individual age ratings within the relevant app store. We also recommend that you download any apps and play them yourself to check their suitability.
• Social Media networks: All social media networks have a minimum age rating; they are all at least 13+.

What else can I do?

• Explain the importance of age ratings to your child.
• Go online together and let your child show you what they are accessing online.
• Set up parental controls on your broadband, devices, consoles and on any individual apps that your child is using. This will reduce the chances of them accessing anything unsuitable as well as viewing inappropriate content for example whilst on YouTube.
• Chat to your child regularly about what they are doing online and as always, remind your child that if anything is worrying them about what they see online then they should tell you or another trusted adult.

What if my child has seen something inappropriate?

This is a useful article from Thinkuknow explaining what to do and who to contact if you have any concerns: https://www.thinkuknow.co.uk/parents/articles/what-to-do-if-your-child-has-seen-something-inappropriate-online/

Cyber Sprinters

This is an exciting interactive online security resources for 7 - 11 year olds. Young people are growing up in an increasingly digital world, exposing them to both the opportunities and risks of the internet. Cyber Sprinters empowers them to make smart decisions about staying secure online.
The digital game can be played on phone, tablet and desktop, and is supported by a suite of activities to be led by educational practitioners working with 7-11 year olds. Parents and carers can also try the Cyber Sprinter puzzles with their children at home!

https://www.ncsc.gov.uk/collection/cybersprinters

Artificial Intelligence (AI)

It can be difficult to keep up to date with new technologies and to know if there are any related risks that we need to be aware of when using new technologies. AI is being talked about a lot, so it is worthwhile learning more about it now to help support/answer questions if our children show an interest. Twinkl provide a brilliant overview of AI here:
https://www.twinkl.co.uk/blog/parents-guide-top-tips-for-navigating-generative-ai-safely-with-kids

How can I keep my child's online accounts safe?

Just like riding a bike, children need to be taught how to use their digital space and how to stay safe. Data breaches can happen to anyone, but children's vulnerability online make them more at risk.

What is a data breach?
According to the National Cyber Security Centre (NCSC), a data breach is when a cyber criminal gets access to information without permission. Criminals usually do this by using their technical skills to hack into computers or websites. If a cyber criminal gains access to your child's details, advises the NCSC, "they can use it to create convincing phishing emails or scam text messages . . . to trick recipients into providing valuable information, such as their passwords."

Advice

Using strong passwords to prevent data breaches

If your child's details are stolen in a data breach, criminals will try and access their accounts by trying the really obvious passwords that millions of people use.

Tips for creating strong passwords

As your child starts to create online accounts, it's important they understand how to choose a strong password.

1. Avoid common passwords that can be easily guessed "This might include a birthday, a favourite team or the name of a family member or pet. This kind of information may exist . . . online, which means they are easy to find out."
2. Use three random words "Choose any three random words and put them together to create a single password. For example, 'apple', 'nemo' and 'biro' could become applenemobiro." These passwords are hard to guess.
3. Use a different password for every account If one account is hacked, the cyber criminal will not be able to access any other accounts if the passwords are all different. Write the different passwords somewhere safe and away from devices, use a password manager or save them in-browser to remember them

Use 2FA

Two-factor authentication, also called two-step verification (2SV) or multi-factor authentication (MFA) helps create more secure online accounts. Using 2FA means that users and cyber criminals cannot login to an account with just a username and password.

How to set up 2FA

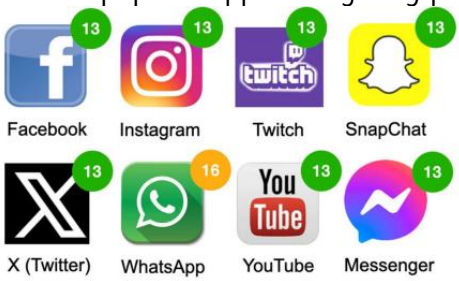
According to the NCSC, "all social media platforms allow you to turn on 2-Step Verification (2SV)." While 2FV is available across platforms, how you set this up will vary. However, you can usually find this setting with these steps:

1. Open the app and go to your account settings.
2. Find the setting labelled 'Privacy and Security', 'Security', 'Account Settings' or similar.
3. Locate 'Two-Factor Authentication' or 'Two-Step Verification' or similar.
4. Follow in-app instructions to set it up. You may need a separate device or email, depending on the app.

For more information, please visit: https://www.internetmatters.org/resources/what-is-cybersecurity/how-can-i-keep-my-childs-online-accounts-safe/

Age Ratings

Age ratings are in place to help protect your child, so we thought we'd provide you with a little reminder of how important it is to check the age ratings of what your child is accessing online. Here are the age ratings of some of the more popular apps that young people are accessing.



It is important to note that whilst age ratings do allow you to see if something may be appropriate for your child, it is also important to review the content yourself. This will allow you to make an informed decision as to whether it is suitable for your child to access and if it would be beneficial to apply further parental controls.

Screen Time

The current world situation means that children and adults alike are all spending more time using devices with screens than we do usually. Whilst we are so lucky that technology is enabling us all to keep working, socialising and learning right now, it is more important than ever to manage and optimise the time we spend using our screens. Not only do we need to make sure we do this for ourselves, our children also need our help to do the same.

Why do we need to manage screen time?

It's common knowledge that the use of screens can impact our health – both physically and mentally. However, it isn't a case of screen = bad and no-screen = good. It's how we use our screens and what we use them for that determines whether they have a positive or negative impact on our lives. Here's a couple of points to consider around why managing screen time is important…

Sitting down too long:

Screen time is usually, but not always, paired with sitting still and inactivity in general. Too much time sitting – and too much time sitting in a bad position, is not good for us physically. It can be bad for posture and lead to weight gain and lower fitness levels.

The solution is to make sure to take regular breaks – we factor in a lot of breaks on all of our online courses to ensure that kids are able to get up, stretch their muscles and get a little bit of activity in, between bouts of learning. Also, we recommend that you are always sitting comfortably whilst using a screen and make sure that your laptop or device is positioned in a way that avoids hand strain or bad posture.

Mindless instead of mindful:

What your child uses a screen for matters – whether that's work or play. Using a screen for socialising or having fun is just as important as it is for learning – especially right now. But the quality of that socialising, playing or learning matters. A video call with a friend or family member is a much better way to use a screen for socialising than using text-based messaging.

A game that helps your child develop skills and learn kills two birds with one stone – and the quality of the education material they are watching makes all the difference when it comes to learning.

Timing is everything:

Using screens just before bed can cause sleep issues. This is because the blue-light being emitted from screens lowers the amount of the sleep hormone melatonin being produced in our bodies, which makes us feel less drowsy, and in turn, makes it harder for us to fall asleep.

It's best to turn on blue-light filters in the evenings when using screens and make sure to stop using screens altogether, a couple of hours before bedtime.

Tips for managing screen time with your children

1. DISCUSS THE PROS OF LIMITING SCREEN TIME WITH YOUR CHILDREN

As parents, it's up to you to make decisions and set boundaries for our kids – but that doesn't mean you shouldn't involve your children in this process. Doing so may mean that your children find it easier to accept the limitations put in place.

2. ENCOURAGE GOOD SCREEN-USAGE

Using screens actively for learning and socialising is healthy screen time. Video calling friends and family, watching videos to learn a new skill or facilitate physical activities – or using a screen to create something like an animation should all be encouraged. However make sure these fit around real-world interactions, sleep, meal times, and similar offline activities rather than the other way round.

3. SCHEDULE IN SCREEN-FREE TIME

Agree, as a family, to have some time each day when screens are entirely banned. Mealtimes and a few hours for bed are ideal times to consider.

4. CREATE SCREEN-FREE ZONES AROUND YOUR HOME

Try making a rule that your kids can only use screens in whatever room you are also in so that you can be aware of what they are doing and this way it will be easier for you to manage their screen time. You could also restrict screen time to only certain rooms i.e. the living room, so that everywhere else in the home becomes a screen-free zone to enjoy other more analogue activities.

Further information

https://www.commonsensemedia.org/screen-time
https://www.internetmatters.org/issues/screen-time/
https://www.internetmatters.org/issues/screen-time/protect-your-child/

Just For Fun

Across

2 = Tell an _____if you see or read something online that you do not like.
3 = When communicating online, I must _____others.
5 = Bullying online is called _____.
8 = Only accept _____requests from people that you know.

Down

1 = I must not share my _____ as I could get hacked.
4 = Hiding behind a fake profile to be unkind is called _____.
6= Online _____ can be good fun with friends.
7 = Do not open unknown emails, as they may contain a _____.