E-SAFETY NEWSLETTER

BPS BALLIOL PRIMARY SCHOOL

October 2024

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/

Parental Controls - Setting up restrictions

Do you have parental controls set up?

Many children have access to technology and the internet through computers, tablets, games consoles, apps and many more things. Parental controls help you to stay in control of what your child can see and do online. Although they can differ from website to app to computer, this website has some great and very easy to follow guides to help you get started:
https://www.internetmatters.org/parental-controls/

https://www.youtube.com/playlist?list=PLJSbhHkqYnrQLoUeeb0lv-5UHiBk-bIf-
(Short how to videos from internet matters)

These websites have some very useful information to help you and your children stay safe when using amazon prime video and Netflix
https://parentzone.org.uk/article/amazon-primeamazon-video

https://parentzone.org.uk/article/netflix-everything-you-need-know-about-streaming-service

You can also use this website to check how old your child needs to be if you are unsure:
https://parentzone.org.uk/article/how-old-does-your-child-have-be

https://www.commonsensemedia.org/

Parent Checklist

Put yourself in control

Make use of the parental controls on your home broadband and any internet-enabled devices. You can find out how at your broadband provider's website or by visiting internetmatters.org.

Search safely

Use safe search engines such as https://www.safesearchkids.com/kids-search-engine/ or https://kids.kiddle.co/Ask.com or http://www.dibdabdoo.com/ or https://kidssearch.com/ .Safe search settings can also be activated on Google and other search engines as well as YouTube. You can find out more at https://safety.google/intl/en_uk/families/

Agree boundaries

Be clear what your child can and can't do online – where they can use the internet, how much time they can spend online, the sites they can visit and the type of information they can share. Agree with your child when they can have a mobile phone or tablet.

Explore together

The best way to find out what your child is doing online is to ask them to tell you about it. Put the family computer in a communal area so you can see what sites they're visiting and share with them.

Check if it's suitable

The age ratings that come with games, apps, films and social networks are a good guide to whether they're suitable for your child. The minimum age limit is 13 for several social networking sites, including Facebook and Instagram.

Online Safety

According to the latest research from Ofcom, nearly half of all 3-4 year olds have their own tablet (Children and parents: media use and attitudes report 2022) so it is never too early to start chatting to our children about how to stay safe online. But how can we do this? Here are some of our suggestions:

- Use books to spark conversations = Childnet have created a collection of five 'Digiduck' stories to help you educate your child (aimed at aged 3–7) about online safety. The stories are available here: https://www.childnet.com/resources/digiduck-stories/ In addition, Childnet have created a learning-to-read book for children aged 4 and above titled 'On the internet.' The book also includes puzzles to encourage conversations. The book can be downloaded here: https://www.childnet.com/resources/a-learning-to-read-book/
- Watch online safety cartoons together = ThinkuKnow have created different animations for different age groups. All you need to do is go to their website and click on the age of your child to get the most appropriate videos https://www.thinkuknow.co.uk/
- ThinkuKnow also provide some useful guidance and advice on what else you can do to keep your child safer online, such as setting up appropriate parental controls.

Keeping Personal Information Safe

With the excitement of a new school year and your child reaching a new milestone, many of us share photos of our child online without thinking about the associated risks. If you post online, then try following these basic rules:

- Don't post any photos of your child that show their school logo/name or recognisable places by where they live that can make it easy for people to find out their location.
- Never include your child's full name.
- Are there any other children in the pictures you share online? If yes, do you have permission from their parent/carer to upload it?
- Would your child be happy for your comment/photo about them to be online – remember what might be 'cute' now may be embarrassing to them in the future.
- Make sure appropriate privacy settings are on.

Alternatively, you could just share photos with those who you really want to share the photo with (grandparents etc.) via WhatsApp or iMessage rather than via social media. Further information CEOP have published this article which includes advice on sharing photos of your child online:

https://www.thinkuknow.co.uk/parents/articles/Sharing-pictures-of-your-children/

Advice on keeping electronic devices out of children's bedrooms

One of the primary issues that phones and electronic devices in bedroom can lead to is **sleep disruption**. Screen time, in general, can be a distraction, but many devices also emit blue light, which has been linked to making it harder for our brains to wind down and relax. By setting a rule that devices do not go into their bedroom (or at least not overnight) you are gaining some control over their online activity. This rule has the added benefit that your child will be less distracted when trying to sleep. According to Natterhub's Data Report **46% of 9-10 year olds admit their sleep is affected by technology**, so by keeping devices safely in your care, it ensures they cannot go online unseen but also reduces sleep interruptions.

To read the Natterhub's data report, visit this website: https://natterhub.com/report2022

Another potential risk is that unrestricted electronic device access in bedrooms also opens up potential dangers for children to encounter inappropriate online content, whether accidentally or deliberately. While a valuable educational resource, the internet also hosts content unsuitable for children, such as violent media, explicit material, or platforms for cyberbullying. Night time browsing, often unsupervised, further increases the risk of exposure. Alone in their rooms, children may venture into unsafe digital territories or interact with unknown individuals.

Cyber bullying

What is it?

It can take many forms, but can go even further than face to face bullying by invading home and personal space and can target one or more people. It can take place across age groups and target anyone. It can include threats and intimidation, harassment, defamation, exclusion or peer rejection, impersonation and unauthorised publication of private information or images. It can include messages intended as jokes, but which have a harmful or upsetting effect.

Some examples of cyber bullying =

- *Text message bullying* involves sending unwelcome texts that are threatening or cause discomfort.
- *Picture/video-clip bullying via mobile phone cameras* is used to make the person being bullied feel threatened or embarrassed, with images usually sent to other people. For example, 'Happy slapping' involves filming and sharing physical attacks.
- *Sexting* involves sending sexually explicit photographs or messages via mobile phone. This can include via text message or by apps such as snapchat.
- *Phone call bullying via mobile phone* uses silent calls or abusive messages. Sometimes the bullied person's phone is stolen and used to harass others, who then think the phone owner is responsible. As with all mobile phone bullying, the perpetrators often disguise their numbers, sometimes using someone else's phone to avoid being identified.
- *Email bullying* uses email to send bullying or threatening messages, often using a pseudonym for anonymity or using someone else's name to pin the blame on them.
- *Chat room bullying* involves sending menacing or upsetting responses to children or young people when they are in a web-based chat room.
- *Bullying through instant messaging (IM)* is an Internet-based form of bullying where children and young people are sent unpleasant messages as they conduct real-time conversations online.
- *Bullying via websites* includes the use of defamatory blogs (web logs), personal websites and online personal polling sites. There has also been a significant increase in social networking sites for young people, which can provide new opportunities for cyberbullying.

Advice for parents:

1. Don't wait for something to happen before you act. Make sure your child understands how to use these technologies safely and knows about the risks and consequences of misusing them.
2. Make sure your child knows what to do if they or someone they know are being cyber bullied.
3. Encourage your child to talk to you if they have any problems with cyber bullying. If they do have a problem, contact the school, the mobile network or the Internet Service Provider (ISP) to do something about it.
4. Parental control software can limit who your child sends emails to and who he or she receives them from. It can also block access to some chat rooms.
5. Moderated chat rooms are supervised by trained adults. Your Internet service provider will tell you whether they provide moderated chat services.

Advice for children:

If you're being bullied by phone or the Internet

Remember, bullying is never your fault. It can be stopped and it can usually be traced.

Don't ignore the bullying. Tell someone you trust, such as a teacher or parent, or call an advice line.

Try to keep calm. If you are frightened, try to show it as little as possible. Don't get angry, it will only make the person bullying you more likely to continue. There's plenty of online advice on how to react to cyber bullying. For example, www.kidscape.org.uk and www.wiredsafety.org have some useful tips.

Text/video messaging

You can easily stop receiving text messages for a while by turning off incoming messages for a couple of days. This might stop the person texting you by making them believe you've changed your phone number. To find out how to do this, visit www.wiredsafety.org.

If the bullying persists, you can change your phone number. Ask your mobile service provider (such as Orange, O2, Vodafone or T-Mobile). Don't reply to abusive or worrying

text or video messages. Your mobile service provider will have a number for you to ring or text to report phone bullying. Visit their website for details. Don't delete messages from cyber bullies. You don't have to read them, but you should keep them as evidence. Text harassment is a crime. If the calls are simply annoying, tell a teacher, parent or carer. If they are threatening or malicious and they persist, report them to the police, taking with you all the messages you've received.

Phone calls

If you get an abusive or silent phone call, don't hang up immediately. Instead, put the phone down and walk away for a few minutes. Then hang up or turn your phone off. Once they realise they can't get you rattled, callers usually get bored and stop bothering you. If abusive, you could report it to your provider or if extreme and persistent to the police. Always tell someone else: a teacher, youth worker, mum or dad, or carer. Get them to support you and monitor what's going on. Don't give out personal details such as your phone number to just anyone. And never leave your phone lying around. When you answer your phone, just say 'hello', not your name. If they ask you to confirm your phone number, ask what number they want and then tell them if they've got the right number or not.
You can use your voicemail to vet your calls. A lot of mobiles display the caller's number. See if you recognise it. If you don't, let it divert to voicemail instead of answering it. And don't leave your name on your voicemail greeting. You could get an adult to record your greeting. Their voice might stop the caller ringing again. Almost all calls nowadays can be traced. If the problem continues, think about changing your phone number. If you receive calls that scare or trouble you, make a note of the times and dates and report them to the police. If your mobile can record calls, take the recording too

Emails

Never reply to unpleasant or unwanted emails ('flames') — the sender wants a response, so don't give them that satisfaction. Keep the emails as evidence. And tell an adult about them. Ask an adult to contact the sender's Internet Service Provider (ISP) by writing abuse@ and then the host, e.g. abuse@hotmail.com

Never reply to someone you don't know, even if there's an option to 'unsubscribe'. Replying simply confirms your email address as a real one

Web bullying

If the bullying is on a school website, tell a teacher or parent, just as you would if the bullying were face-to-face. If you don't know the owner of the website, follow one of the online safety links below to find out how to get more information about the owner.

Chat rooms and instant messaging

Never give out your name, address, phone number, school name or password online. It's a good idea to use a nickname. And don't give out photos of yourself. Don't accept emails or open files from people you don't know. Remember it might not just be people your own age in a chat room. Stick to public areas in chat rooms and get out if you feel uncomfortable. Tell your parents or carers if you feel uncomfortable or worried about anything that happens in a chat room. Think carefully about what you write; don't leave yourself open to bullying.

What are the top tips? Three steps to stay out of harms way =

1. Respect other people - online and off. Don't spread rumours about people or share their secrets, including their phone numbers, passwords, photographs and videos.
2. If someone insults you online or by phone, stay calm – and ignore them.
3. Do as you would be done by.' Think how you would feel if you were bullied. You're responsible for your own behaviour – make sure you don't distress other people or cause them to be bullied by someone else.

Cybercrime

From phishing scams to online fraud, hacking and ransomware attacks, we're all susceptible to cybercrime, but protecting your kids against it is inherently tricky. They're part of a digital generation that relies on online messaging platforms, social media and the Internet to communicate with friends, learn and play. Cyber criminals are more inclined to hunt down vulnerable targets, and young children can be more easily tricked into giving up personal data or their parents' financial information. Kids are curious online, but they can also be overly trusting and more naïve than adults. With that in mind, it's vital you take steps to protect your children from cybercrime.

Here's some practical tips:

1. Talk to them!

It's important to start the conversation about cybercrime. By raising awareness of the darker side of the Internet, you'll be committing both yourself and your children to safer online practices. There's no need to scare them, either. Learning about cybercrime can be fun and interactive. For example, the SafeKids Online Safety Quiz is a great way to get them thinking about cybercrime without putting them off using the Internet entirely. https://www.safekids.com/quiz/

2. Work together on their online identity

It's important when choosing usernames and passwords for online services that you don't use information that might identify you or be easy for hackers to guess. Teach your kids about the importance of complex passwords by working together to create theirs. Go for passwords of at least eight characters in length that include numbers, letters (both upper and lower case) and symbols. Finding appropriate and non-identifying usernames can be made fun, too, by playing word games to see who can come up with the most inventive.

3. Teach them the basic techy stuff

Kids love to learn, and you can use this to your advantage when teaching them about online safety. If you come across a potentially malicious website or email during your own time online, show them what made you suspicious (providing the content is appropriate, of course). It's also important to show them some of the techy elements of the web that help raise awareness about online safety. For instance, looking for 'https' at the beginning of web addresses (the 's' stands for 'secure' and means all traffic between the web browser and and website is protected to industry standard) and the presence of the padlock symbol are important skills in the digital age.

4. Discuss what should and shouldn't be shared

We live in a sharing culture, and your children will be inclined to share stuff far and wide if they think it's interesting, funny or likely to impress their peers. Unfortunately, that means the wrong type of information and images often get shared. This is why it's important to talk to your children about what they can and can't share. Your address, telephone numbers and certain types of photography (family photos and those that provide an insight into your home security, for instance) should be kept at bay, but there's no harm in them sharing content they find which is harmless or educational.

5. Bonus tip: Try using a child-safe browser

Modern web browsers are packed full of clever technology that enables parents to tightly lock down the ability for their children to access unsavoury content and protect themselves from online crime. Despite this, it might be easier to check out some of the child-safe browsers. These have such security built-in and turned on by default, and that means you'll spend less time working out how to configure the browsers you use.

For more information, you can read more here:
https://www.voicenorthants.org/2018/02/teach-kids-cybercrime-without-scaring/