Parkfield School

Hurn
Christchurch
Dorset
BH23 6DF

Email: office@parkfield.bournemouth.sch.uk
Website: www.parkfieldschool.org
Telephone: 01202 592530
Principal: Mr. Ian Golding

3rd April 2020

Dear Parents/Carers,

Re: Safeguarding Children Against Online Harm

Now that the vast majority of school-age children are at home owing to school closures, it is important to make sure they are *safeguarded against online harm..*

Here are the three main reasons:

- **Having more free time on their hands** – as well as more time participating in distance learning – they are more vulnerable to situations such as stranger danger, stumbling across inappropriate content, being the targets of various forms of abuse or inadvertently facilitating malware.

- **Cybercriminals are exploiting the crisis** with a huge volume of emails, texts, social media posts and phone calls seeking to commit fraud or identity theft.

- **You have many other things to worry about:** safeguarding yourself and your loved ones in the physical world, protecting your income, and if you're normally office-based, trying to get used to working and meeting remotely and maintaining business as usual.

It is always important to do whatever you can to protect your children in the online world, but now, the risks have increased. Please take time to read the advice at **getsafeonline.org/safeguarding-children** to make sure they are protected as much online as they are from Coronavirus.

Remember: having regular, ongoing conversations with your children about what they're doing, who they're talking to and what apps they're using is equally important as tech solutions such as parental controls or ISP filters.

SANS – a globally-respected cybersecurity solutions and training provider, has made some of its valuable resources available free of charge in the face of the current Coronavirus pandemic. It's just over four minutes but could help you protect your child.

Advice if your child is under 5 years old

- Start setting some boundaries, even at this early age … it's never too early to do things like setting limits for the amount of time they can spend on the computer.
- Make sure devices like your mobile, tablet or laptop are out of reach. Set up passwords/PINs and make sure you keep these details to yourself.
- On computers and any other devices your child has access to, set the parental controls to the appropriate age, and enabling access to only appropriate content.

- Buy or download parental control software, switch it on and keep it updated. There are many versions on the market, which work in different ways and available at a range of prices, starting at free.
- The big four Internet Service Providers (ISPs) give their customers free parental controls which can be activated at any time. Check them out and take advantage of them.
- Buy or download only apps, games, online TV and films which have age ratings, which you should check before allowing your child to play with or watch them.
- Share your technology rules with grandparents, babysitters and your child's friends' parents so that they know what to do when looking after your child.
- When using public WiFi – for example in cafés or hotels – remember that it might not include parental controls. Innocently letting your child play with your mobile or tablet while you're enjoying a latte may result in them accessing inappropriate content or revealing personal information.
- If you have a family computer or tablet, set the homepage to an appropriate website such as Cbeebies

Advice if your child is between 6 - 9

- On computers and any other devices your child has access to, set the parental controls to the appropriate age, and enabling access to only appropriate content.
- Buy or download parental control software, switch it on and keep it updated. There are many versions on the market, which work in different ways and available at a range of prices, starting at free.
- The big four Internet Service Providers (ISPs) give their customers free parental controls which can be activated at any time. Check them out and take advantage of them.
- Agree a list of websites your child is allowed to visit and the kind of personal information they shouldn't reveal about themselves online, such as the name of their school or their home address.
- Set time limits for activities such as using the internet and games consoles.
- Make sure your child is accessing only age-appropriate content by checking out the age ratings on games, online TV, films and apps.
- Discuss with your older children what they should or shouldn't be showing their younger siblings on the internet, mobile devices, games consoles and other devices.
- Discuss with other parents, subjects such as what age to buy children devices that connect to the internet.
- Don't be pressured by your child into letting them use certain technologies or view certain online content, if you don't think they are old enough or mature enough… no matter how much they pester you or what their friends' parents allow.

Advice for 10 – 12 year olds

- Set some boundaries for your child before they get their first 'connected device' (mobile, tablet, laptop or games console). Once they have it, it can be more difficult to change the way they use it or the settings.
- Tell your child that it's very important to keep phones and other devices secure and well hidden when they're not at home, to minimise the risk of theft or loss.
- Discuss with your child what is safe and appropriate to post and share online. Written comments, photos and videos all form part of their 'digital footprint' and could be seen by anyone and available on the internet forever, even if it is subsequently deleted.
- Talk to your child about the kind of content they see online. They might be looking for information about their changing bodies and exploring relationships. They also need to understand the importance of not sending other people - whoever they are - pictures of themselves naked.

- Remember that services like Facebook and YouTube have a minimum age limit of 13 for a reason. Don't bow to pressure, talk to other parents and their school to make sure everyone is in agreement.
- Explain to your child that being online doesn't give them anonymity or protection, and that they shouldn't do anything online that they wouldn't do face-to-face.

Advice for 13 years and older

- It's never too late to reinforce boundaries … your child may think they are adult enough, but they definitely still need your wisdom and guidance.
- You may be starting to think your child knows more about using technology than you do, and you may be right. Make it your business to keep up to date and discuss what you know with your child.
- Talk frankly to your child about how they explore issues related to the health, wellbeing, body image and sexuality of themselves and others online. They may be discovering inaccurate or dangerous information on online at what is a vulnerable time in their lives.
- Review the settings on parental controls in line with your child's age and maturity and adjust them if appropriate. They may ask you to trust them sufficiently to turn them off completely, but think carefully before you do and agree in advance what is acceptable online behaviour.
- Also talk frankly to your child about how they behave towards others, particularly with regard to what they post online. Be willing to have frank conversations about bullying, and posting hurtful, misleading or untrue comments. Make them aware of the dangers of behaviours like sexting and inappropriate use of webcams.
- Give your child control of their own budget for activities like downloading apps and music, but agree boundaries beforehand so that they manage their money responsibly. Don't give them access to your payment card or other financial details.
- Be clear in your own mind on issues such as copyrighted material and plagiarism so that you can explain to your child what is legal and what isn't.
- If your child has the technological know-how – and with sufficient influence from others – they could be vulnerable to experimenting with accessing confidential information from the websites of other people or companies. Hacking amongst this age group is very rare, but it does exist. Explain the dangers and consequences.

We hope this guidance will help to ensure that we are doing our upmost to keep our children safe online. For further information, please refer to the resources attached.

Kind regards

Miss T. Wilcox
KS2 Lead