Friday 10th May 2019

Dear Parent/ Carers,

Following our first e-safety newsletter last term, we have gathered some advice and guidance from e-safety organisations on age restrictions, screen time and phishing.

Age restrictions

Many parents often ask how old their child has to be in order to use social media legally. The answer is they have to be the age stated in the terms and conditions of the host app/website. Here is a summary of the minimum age required by the better known social media companies:

Social Media	Age Requirements
WhatsApp	16 (in the EU)
YouTube	18 to have your own account or channel, but this can be 13 with parental permission.
Instagram	Minimum age of 13
TikTok	Minimum age of 13
Snapchat	Minimum age of 13

The age restrictions are in place to protect children from such issues as data protection risks, cyber-bullying and online harrassment. Online safety researchers believe that children's cognitive structures are not developed enough to see the risks of their actions in an online environment until the age of thirteen, regardless of how tech-savvy they are. It is important that parents and carers are aware of the dangers social media can cause when children are not aware of the consequence of their actions in an online environment.
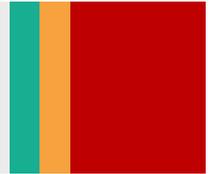
Screen Time

Screen time is an issue being discussed a lot in the news at the moment. There is a lot of discussion about how much screen time is healthy. If parents or carers do ask about their child's screen time, as always, the best advice to give is to encourage open and honest conversations with their child about their internet use. If they are still concerned, most devices such as iPhones, Samsung, PlayStations and Xboxes now have parental controls that allow for the limiting of screen time. A quick search online brings up plenty of guidance the parent/carer can follow to make use of these. Internet Matters has some very good guidance on Parental Controls: https://www.internetmatters.org/parental-controls/. Recently, Apple have brought out some excellent guidance on how to use parental controls and manage screen time on their devices: https://support.apple.com/en-gb/HT201304.

Ofsted
Good Provider

Phishing and the Secure Padlock

Good advice to children is to always check the web address bar to see if it has the little padlock on the left hand side and the web address starts with 'https', with the **s** denoting secure. However, security researchers are finding that criminals are also using the padlock in the hope that the audience will be tricked into thinking the site is legitimate and/or safe. Therefore, whilst it is still good advice to check for a secure connection by looking for the padlock and https, users should also check:

- Grammar and spelling (this is the easiest and the most common to find).
- Suspicious popups making outlandish claims (e.g. win an iPad).
- A slight alteration to the web address (an obvious one might be Barc1ays, where the L has been changed to a figure 1).

If you have any further questions or would like to find out more about the subjects covered in this letter, please follow the link below to Safer Internet, which outlines clear advice and information about keeping children safe online.

https://www.saferinternet.org.uk/advice-centre/parents-and-carers

Thank you for your continued support.

Yours sincerely,

Miss Kilby