Below is some of the latest Cyber Safety guidance that has been passed onto us from our local PSCOs who specialise in Cyber Safety

- Strong Passwords now should be 12 – 16 characters long, we recommend they are made up of 3 or 4 words chosen at random and a password for each account, these prevent daisy chain attacks where offenders break one password and then have access to all that persons accounts due to a recurring password.

- Parents/Carers should know their children's passwords. To help remember all passwords you can use a Password Manager Service.

- When gaming children should utilise 'Two Factor Authentication' as an extra layer of security. This can be set up on Playstation and Xbox. Children should play games suited to their ages as defined by PEGI. A number of sites provide further reviews of game suitability, including:
  Game Reviews - Kids Games | Common Sense Media
  askaboutgames.com

- On apps and when gaming, Privacy settings should be used, with the option 'Friends Only' selected and these should be friends who children know and trust in real life, as well as approved of by Parents/Carers. Gamers should ensure that their Usernames do not reveal personal information and so, similar to passwords, they should be chosen using words chosen at random.

- There are occasions where children sometimes encounter Cyber Bullying, it is important that children understand how to Mute, Block and together with Parents they can Report to the administrator of the site. See how here:
  www.nationalbullyinghelpline.co.uk/social-media
  Please the school know if your child has experienced Cyber Bullying. It can also be reported to the police.

- In terms of Social Media, we are aware that pupils as young as Year 3 have their own Tik Tok accounts. We would suggest that pupils adhere to the age limits of Social Media apps e.g. Tik Tok, Snapchat, Instagram, Twitter – 13 years old. Once again these accounts have privacy settings and when we speak to older children who are allowed on such apps we always advise them to select friends only, taking care not to accept people they don't know. They are also advised about not revealing their location and to utilise services such as Ghost Mode if on Snap Maps. If Parents/Carers have doubts about app suitability then there a number of sites which can help including:
  App Reviews - Kids Apps | Common Sense Media.
  Two Factor Authentication can also be used on many Social Media accounts.

- **We would just reiterate that we suggest that children wait until they are 13 years of age before using Social Media accounts.**

- Whether gaming or on apps, children should be wary of not revealing personal information and have a clear understanding of what personal information would be. Sometimes small amounts of personal information gets revealed over a period of time, for example when playing online over a few weeks through direct chat or messaging. On many games Chat functions can be turned off.

- Linked to many games is the capacity for 'In app purchases', some children have been able to run up big bills, so it is important that Parents/Carers are vigilant to the capabilities of different apps and the access children may have to financial accounts.

- Limiting the amount of time that children are online and indeed playing games can be a real challenge for Parents/Carers, particularly for Parents of children who have SEN. Rather than putting time limits in place many Parents are finding that it is more productive to consider game time from the perspective of the child completing levels. This allows the child to complete the level and comprehend that the activity has come to an end, avoiding escalating conflict within the home.

- Parents/Carers can use Parental Controls to make children's online experience safer. 02 & NSPCC have launched a helpline which Parents and Carers can ring for guidance on setting up Parental Controls and other online safety advice. You do not need to be an 02 customer to access the helpline (0808 800 5002).

- Many Junior School pupils are now being given their own Smart Phones. Children should be taught to be wary about scam calls including scam text messages or emails urging the user to click on a link. Similar to adults, children need to be wary of clicking on links or downloading attachments unless they are certain of their validity, as it can allow offenders to take control of devices.

Other websites that you may find useful include:
www.thinkuknow.co.uk
www.nationalonlinesafety.com
www.saferinternet.org.uk
www.nationalbullyinghelpline.co.uk
If you have twitter you can also follow twitter.com/GlosSaferCyber