Cyber Safety

Over the last 20 years, we have become increasingly reliant upon the internet and the myriad of technological advances that have accompanied it.

However, whilst the internet affords us tremendous opportunities for children to learn and have fun, it is vital that as parents we empower them with the skills and security measures to help them navigate this virtual world safely.

Below are some of the latest Cyber Safety guidance that parents and carers should be aware of to help keep children safer online:

Passwords – We hear so often that Passwords should be strong, but often parents are left bemused about what that actually means. The latest advice places more of an emphasis on length rather than complexity. So for example, a password such as Greenconcretetrousers would be stronger than U3*&d5#b

When choosing a password, use three or four words selected at random. Ensure they are in no way inspired by your interests or family life which could be guessed by someone.

Have a different password for each account in order to prevent 'daisy chain attacks' where offenders break one password and then have access to all that persons accounts due to a recurring password.

It can be helpful for parents/carers to know their children's passwords. With so many different accounts that can soon become quite a long list. Many people are finding it much easier to use a Password Manager Service. There are a number of these on the market and some are free.

To add an extra layer of security when on social media or when gaming, children can benefit from having 'Two Factor Authentication' in place. Step-by-step guidance for turning this on can be found at www.authy.com.

Children benefit from playing games that are suited to their age group. Rating agency – PEGI provides age appropriate guidance for games. (Home | Pegi Public Site). A number of sites provide further reviews of game suitability Game Reviews - Kids Games | Common Sense Media and Home (askaboutgames.com)

On gaming and social media apps, Privacy Settings should be used, with the option 'Friends Only' selected and these should be friends who children know and trust in real life, and be 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 selected at random.

There are occasions where children sometimes encounter Cyber Bullying, it is important that children understand how to Mute, Block individuals and together with parents they can Report to the administrator of the site. Further advice on Cyber bullying can be found here: Helping Children Deal with Bullying & Cyberbullying | NSPCC

Increasingly, more and more children under ten years old are 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 or download malicious software such as viruses.

In terms of Social Media, we are aware that even very young children are using services designed for those over the age of 13, such as TikTok, Snapchat and Instagram. These platforms can contain content that is not suitable for young children, so we would advise all parents and carers to wait until your children are at least 13 years old before allowing them to open an account.

We know many young people accept friend / follow requests from people they don't know – it is vital young people know that not everyone online is who they say they are, so they should avoid this. Many social media platforms also use location services, such as Snapmaps on Snapchat, these can reveal a young person's location so we would strongly advise parents to check their children's settings to keep them safe. If parents/carers are unsure if an app is suitable for their children, there a number of sites which can help including App Reviews - Kids Apps | Common Sense Media.

Whether gaming or using 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 and carers. Rather than putting time limits in place, some parents and carers find 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 and carers can use Parental Controls to make children's online experience safer. 02 & NSPCC run 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 which is available on 0808 800 5002. Alternatively, visit Parental Controls & Privacy Settings Guides - Internet Matters

Overall, parents and carers benefit from being part of their children's online lives, whether that be gaming together or just ensuring they know that should they ever have a problem online you are there to support them. Digital Parenting is here to stay.

In the event that something does go wrong online, Schools now have a great deal of experience in online safeguarding and many parents and carers have made good use of the advice and guidance available within School Pastoral Teams.

With regard to contacting Police – if it is an emergency then parents/carers should call 999, if not, then call 101.

From a local perspective, the Police Community Support Officers (PCSOs) are engaged with their communities providing advice and guidance on a whole range of crime prevention matters including Cyber Safety. Please see link below to contact your PCSO:

Contact us | Gloucestershire Constabulary