The Chiltern School
Online Safety

Chatting

Children can talk to others online in a variety of ways using many different platforms – this can be via text-based messaging, including instant messaging and SMS, or voice/video link, including internet phone calls and webcam. Chatting can also take the form of instant, real-time communication through chat rooms and instant messaging, or delayed communication using email and voicemail.

Tips for parents:

• Familiarise yourself with the chat programme your child uses and make sure you understand its safety functions, such as passwords, privacy settings or parental controls – contact the service provider if you are unsure.

• Make sure you talk to your child to find out who they are talking to online – encourage them to think before talking to anyone they don't know in person.

• Make sure your child understands that not everybody is who they say they are online. Explain that in some cases profiles may be people posing as someone they aren't (e.g. an adult posing as a child) or may be "bots" (which are automated software programs designed to create and control fake social media accounts).

• Pay attention to and monitor your child's online behaviour – make sure you negotiate and establish boundaries, highlighting the importance of the concept of online 'friends', fake profiles, bots and accepting unknown friend requests.

• Make sure your child understands that arranging to meet with anyone they have met online is dangerous, and that they should only do so with your permission.

• Ask your child if they know how to block or remove someone that they don't want to talk to – if they don't, make sure you learn about this and show them. Ensure they know how to report someone who makes them feel uncomfortable online. CEOP (https://www.ceop.police.uk/safety-centre/) is a commonly used platform to report users online.

• Consider installing parental control software to introduce filtering options, monitoring and time limits for access to online chat.

• If you notice any misconduct between your child and someone else, investigate it. Report people and inappropriate conversations to the site provider, and always keep a copy of the conversation as evidence.

• Discuss with your child how people may use chatting to explore their sexuality, e.g. through sexting.

• Explain to your child that some online behaviours are abusive. They are negative, potentially harmful and, in some cases, illegal. Explain the types of online abuse that could occur, e.g. sexual harassment, bullying, trolling and intimidation. Make sure children know they should tell you as soon as possible if they experience abuse or inappropriate contact whilst they're online.

Sharing

Children can share almost anything online – whether this be imagery, videos, opinions and thoughts, interests, or personal details – and all at the click of a button. Whilst this ease of use is widely supported, the risks associated with this also need to be managed.

Tips for parents:

• Consider setting up a family email address and only use this to fill in any online forms requiring personal details.

• Establish clear guidelines for your child so they understand what is suitable to share online and what is not – perhaps give examples of what you have shared online and why.

• Talk to your child about how easy it is for people to assume another identity online.

• Explain that children are sometimes targeted to access adults' data, for example, passing on their parents' details (bank details, date of birth, national insurance number etc).

• Identify and list any sites you wish to block access to – contact your internet service provider if you need to install parental controls.

• Ensure you understand that children can access the internet through publicly available WiFi, such as in restaurants and through mobile data (3G, 4G). Check whether your child's devices have any tools to manage inappropriate content from this access.
• Be aware that some devices contain location technology allowing the device's location and surrounding services to be identified. This also allows the location of the device, and your child, to be identified by others.
• Ensure your child understands that privacy settings have limitations, for example, they will not prevent someone else sharing something inappropriate.
• Inform your child that accepting friend requests from users could enable them access to their profile picture, location, posts and photos.

Gaming

Online gaming is increasingly popular amongst children and can be accessed via mobile phones, computers, games consoles and other devices such as tablets. Through online gaming, children are able to interact with others, including people they don't know, and engage in chatting and sharing.

Tips for parents:
• Access the PEGI guidance (https://pegi.info/page/pegi-age-ratings) on age ratings to inform your choices when buying games for your child, or deciding whether the games they are playing are appropriate, by following the age-ratings assigned to each game.
• Read each game's advice for parents and play the game yourself to help you understand what it involves.
• Explain to your child the reasons for age-restricted games (e.g. they may contain disturbing material not suitable for young users).
• Only allow your child to play games from reputable and legal online providers.
• Determine boundaries for the amount of time your child can spend on online gaming – in particular, regular five-minute breaks taken every 45-60 minutes can help their wellbeing.
• Make sure your child is aware that most games and platforms are businesses designed to make money. They encourage users to stay online in order to encourage them to spend money in the game (e.g. in-app purchases).
• Install parental controls on game consoles to disable or restrict access to facilities, such as voice chat, or to prevent online credit payments.
• Talk to your child about protecting themselves when gaming – keep personal information private, only play games with people they know, etc.
• Make sure your child knows how to report abusive chat when using the game.
• Familiarise yourself with the game's safety functions – contact the service provider if you are unsure.

Content providing

Children are at risk of being exposed to illegal, inappropriate or harmful material; for example, pornography, fake news, racist or radical and extremist views. Similar to sharing, content providing involves files that can be accessed when using the internet and which can potentially harm others, such as viruses that take personal details and pass them on to others.

Tips for parents:
• Install safe search filters and apply these to devices.
• Ensure your child is aware of what 'cookies' are, how their data is 'farmed' in order to target marketing, and let them know about their rights under data protection legislation.
• Check with your internet provider or online security provider to see how you and your child can stay one step ahead of cybercriminals. Internet providers can help you and your child spot suspicious content and avoid malware.
• Make sure your child knows it's illegal to download most films, songs and games without paying for them.
• Point your children to secure sites where they can buy music and films, such as iTunes or Amazon. You can limit the amount they spend by getting them gift cards for a sum.
• Check any download site your child is using and make sure it's legal and trustworthy.

• Consider installing parental controls to monitor your child's browsing and access to certain sites. For those under 18, parents can contact mobile service providers to install network filters that block certain websites.
• Check your child's internet search history for signs of illegal activity – remember, a total lack of internet history may also be a sign of illegal activity.
• Install software filters on all computers, laptops, mobiles and other devices. Similarly, make sure you install antivirus or firewall software on all devices, and keep these up-to-date.
• Check your bank accounts and all bills you receive for any signs of identity theft.
• Discuss how others may explore their sexuality through content providing, e.g. by accessing pornography.
• Find out what plagiarism rules your child's school employs through a discussion with your child or with the school, to understand how to avoid plagiarism.
• Give your child access to legal streaming platforms such as Netflix and Spotify which allow unlimited streaming, if possible.
• Teach your child to spot fake or illegal streaming sites, if something mentions "free", or terms like "unlimited movie streaming" and "100 percent legal", they usually lead to pirated content.
• Much of the information seen online is a result of some form of targeting. Explain to your child that a company pays to be advertised on the platform and aims to catch their attention.

Networking

The use of social networking platforms is popular for several reasons and, whilst it allows children to communicate with others and share their information, it is these actions that pose harmful risks. You should be able to recognise the risks networking can have on your children and aim to communicate with them to better understand what they are doing.

Tips for parents:
• Regularly communicate with your child to find out who they are talking to online, for what purposes, and using which platforms.
• Set boundaries for your child on when they can set up certain social networking accounts and do it with them when you allow this. Make sure your child applies the strongest privacy settings to their social networking accounts. Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared.
• Explain the importance that your child is truthful about their age online to ensure they can only see content suitable to their age – particularly when signing up for social networking sites. Many sites are bound by legislation that may restrict access to underage users.
• Discuss the information that is suitable for them to post on social networking sites, and that they should remember what is posted is retrievable in future.
• Online challenges acquire mass followings and encourage others to take part in what they suggest. While some may be fun and harmless to take part in, others may be dangerous or even illegal. Ensure your child understands when it is safe to share and participate in online challenges and when it may dangerous to do so.