



Online Safety

Introduction

Whilst the use of computers and phones to access online material can be incredibly useful and enhance a child's education, it can also cause serious damage to mental health and relationships. The issues outlined in this document also affect adults.

Monitoring how your child accesses online material can be frustrating; it takes knowledge, time and persistence.

This document provides guidance on online safety relating to how children access some of the most well-known social media platforms and browsers for searching content on the Internet.

Although it is vital to stay up to date with the latest developments and to understand the contents of this document, the most effective way of ensuring your child's safety is still to talk to them openly and honestly about their lives online, without judgement. This will allow you to help them on their journey to becoming a safe user of the internet. Just like all social interaction, children will learn from their mistakes. It is important that they are able to make those mistakes in a supportive environment, with trusted adults to help them if things ever go wrong.

E-safety

Understand what your child has access to when using devices and understand what they may be able to access. Put filters in place if you deem exposure to be of concern or consider restricting use completely.

Remember that even with social media accounts set to private, the main feed is likely to be visible which means that your child can see what the public uploads.

Be mindful that time restrictions can also be placed onto a device, restricting when and how long your child uses the device.

Device management is often very extensive and if you wish to do something specific the likelihood is that you can achieve it. Strive to search out methods that suit your needs (Google and YouTube are excellent resources for this).

Establishing trust and being able to talk to your child about the Internet and social platforms (and for them to be able to talk to you) is possibly the most effective approach anybody could take.

Internet

The Internet is a place of opportunity, inclusion and diversity, the benefits of which outweigh the drawbacks.

Some of the risks are outlined in this document, some severe, but unlikely; others are mildly damaging and frequent.

It is the behaviour of individuals, combined with the vulnerability of children, that may cause issues.

Likewise, the Internet exposes us. It does not change us. Somebody writing negative comments exposes themselves; it is not the technology changing our behaviour.

Inapproapriate Content

Inappropriate content can be searched for but a child may simply stumble upon it accidentally, or it may be shared directly with them by somebody else.

Inappropriate content can come in many other forms, such as through negative comments on social media platforms, chain mail in WhatsApp conversations friend requests from strangers.

How children interact with online content should also be given equal consideration. For example, a completely private TikTok account could still make a child feel insecure about their own appearance through the use of the beautification filters generated as part of the app. Another example is a child misinterpreting a comment, or writing a comment that is read by the recipient in a way that was not intentional.

Example of areas for conecrn

- Access to inappropriate content
- Negative comments made on social media platforms such as Facebook, including apps such as TikTok and WhatsApp
- The way beautification photography filters warp the way children see themselves
- Overuse of mobile phones which breeds laziness, a detachment from reality and dependency
- Fear and anxiety generated through pressure to engage with chain mail, as often seen on apps such as WhatsApp
- Grooming
- Seeking validation through likes, followers and comments on social media (it is interesting to note that, as a pilot, Instagram recently removed all likes from its platform in Australia in an attempt to improve the mental health of users, and this may be rolled out across the platform)

How can I ensure my child is safe online

Please note that the instructional examples below given relate to iPhone for mobile devices. The guidance may be the same/similar on Android and desktop versions.

Examples are given for some of the most common platforms but not every platform is mentioned in this document. All principles apply across all platforms.

Understanding Risks

Establishing trust and being able to talk to your child about the Internet and social platforms (and for them to be able to talk to you) is possibly the most effective approach anybody could take.

As humans, we are naturally curious. Do not let your expectations of your child block the likelihood that at some point they may want to access inappropriate material simply out of curiosity, as may their friends.

Do not underestimate the volume and extremity of inappropriate content available online.

It is vital that you acknowledge your child is at risk, however small the risk may be, even if they do not have access to a mobile phone or computer, simply because of the prevalence of both the Internet and electronic devices. Ignoring the issues or treating them as trivial could result in your child being exposed to something that causes them significant distress.

Managing Expectations

- Children will probably find ways around your controls if they want to, so building trust is highly important.
- Threatening to remove devices from children is unlikely to build trust and encourage children to share negative experiences.
- No matter what safety measures you put in place, children will inevitably encounter adult/inappropriate
 content as they get older. What will they do when this happens? Will they come and talk to you? Will they be
 too embarrassed/scared?
- When talking to children, it is important to show a real interest, and not to dismiss online activities as less valid/important.
- Discuss screen time in a nuanced and positive way (instead of "children spend too much time looking at screens", try "some online activities are more beneficial than others"). There is no evidence that screen time itself is a problem, but that repetitive and negative activities, combined with lack of sleep and time to be mindful have an impact. A useful reference point is https://www.childrenscommissioner.gov.uk/ourwork/digital/5-a-day/). And consider what they would be doing instead.
- Remember that messaging on social media apps is a part of how young people socialise and is not separate from
 it. It is important that parents understand this and approach the subject without too much judgement: children
 will open up and share if they feel able to. Chatting in 'real life' is not intrinsically more valid than
 communicating online.

Treat computers and mobile devices differetly

The way mobile devices are used is very different to the way a computer is used (such as desktop PC or laptop). This is because a mobile device is completely portable and treated as a highly personal possession - particularly a mobile phone. As such, it is often used in a completely different way. A child is more likely to exercise their curiosity on a mobile device and do this in the privacy of their own bedroom, for example. A child will also engage with many more platforms that are only available on mobile devices.

If your child has access to a mobile device and a computer, consider how they use each one and why.

A home computer is more likely to be used as a family computer and based in a static location, in which case a child is more likely to be more reserved in their use of it. The browser (such as Chrome, Firefox or Internet Explorer) may be used as an educational tool and little else (searching for homework-related topics, playing games etc.).

A mobile phone, for example, is much more likely to be used to access social apps, such as WhatsApp, TikTok, Facebook and Snapchat.

How to know what your child is accessing

Each time you search for something online (using a browser such as Internet Explorer, Chrome, Firefox or Safari, for) information relating to what you searched for and any websites you visited is stored in the browser's history. This applies to any device. Your child is unlikely to know how to clear the history of a browser.

- Your browser may show 'History' as a tab. Or it may be hidden in a menu (for example, accessible by clicking 3 small dots at the top far right of the screen in some browsers). Access the history to view activity. If you are logged into Google when the browser is being used (Google Chrome), the history will also be stored in your Google account and therefore accessible to you from your Google account and not tied to that specific device.

It is possible that your child does know how to clear history, so an absence of reference to anything significant does not necessarily mean that they have not seen something inappropriate.

As your child gets older, it would be appropriate to allow more apps on your child's device. However, this must be accompanied by mutual trust - you should feel confident that they will tell you if anything bothers them, and they must trust that you will react in a reasonable and balanced way. For example, if your response to them showing you something inappropriate on their device is shock, outrage or punishment, they are unlikely to make further disclosures.

You can prevent apps (and purchases) being downloaded in the first instance by:

Social Media

Any information that is communicated via a social media platform can be visible to members of the public unless you ensure the relevant privacy settings are in place.

For example, if you have a Facebook account, is your profile public? Many profiles are public without the account holder being aware, and posts and images are available for anybody to look at.

Information that is sent privately could also be brought into the public domain simply because the information can be copied (such as images captured as a screenshot) and posted elsewhere by the recipient.

It is worth nothing that aside from safeguarding concerns, employers now use searches to look for information relating to candidates.

Summary

This applies to any platform that is being used online and on any device:

Top Tips

- Consider who could find your child online and how they could communicate with them.
- Consider what information is being engaged with and shared by your child.
- Consider if the platform is appropriate or not.
- Consider the possible harmful effects of platforms that beautify your child. Set parental filters.
- Set privacy settings.
- Turn off commenting (could be restricted to friends only).
- Explain how comments work and how comments online are different from face-to-face comments.
- Turn off friend requests (could be invite only).
- Do not engage with chain mail.
- Do not focus on getting likes and followers.
- Be mindful of the amount of time being spent online and the purpose it is serving.
- Be open with your child and have regular conversations about online activity.
- Check your child's online activity regularly, including browser history and chat messages.

Some useful websites

Parentzone (digital family advice)

https://parentzone.org.uk/home

Childnet (keeping children safe online)

https://www.childnet.com

NSPCC (preventing abuse)

https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/onlinesafety

Netaware (specific advice about apps and websites) https://www.net-aware.org.uk/

ThinkUKnow (online education programme, aimed at teachers)

https://www.thinkuknow.co.uk/