

How can I help my child stay safe when accessing the internet on their device?

Many devices, such as tablets (e.g. iPad or Kindle Fire) and internet-enabled media players (eg. iPod Touch), connect to the internet to enable a wide range of functions. The same advice that you give your child about keeping safe online applies to these devices, so talk to your child about the SMART rules.

These devices can be easy for young children to use, but this does not necessarily mean they're ready to use them. It is worth bearing in mind that children, especially younger children, can be upset and distressed if they come across age-inappropriate material. Parental controls can be a real help and may be particularly important for younger children. For older teens it can also be a help, but it may be more appropriate to talk about dealing with peer pressure to share and watch content that is inappropriate rather than just simply blocking access to YouTube, for example.

There are several options to help limit internet capability on these devices, so it is worth considering what would help. However, remember that filtering is only part of the solution and it is important to talk with your child about how they use the internet on their device and make sure they know what to do and that they can turn to you if they get into any difficulty.

The iPad and iPod Touch connect to wifi networks, such as your home internet or a wireless hotspot in a coffee shop or library. All of the major internet providers offer free filtering tools that work across all devices connected to the home internet. See our handy video guides from BT, Sky, Talk Talk and Virgin Media. If you're connecting to a public Wi-Fi hotspot look out for the Friendly WiFi symbol which shows that internet filters are in place.

With an iPad, you can also sign up for a 3G contract so that you can access the internet anywhere. Speak to the mobile operator you have a contract with to see if they have any options for filtering the internet.

Some apps can help filter out age inappropriate content or help restrict some functions; have a look in the app store.

Some devices may have options for restricting the internet. For example, it is possible to switch off the Safari browser on the iPad or iPod Touch to prevent these devices from being used to surf the web (see iPad, iPod Touch or Kindle Fire tips).

What should I do if my child has seen something inappropriate?

Don't overreact if your child tells you about something they have seen. It is great they have turned to you as a trusted adult. You might feel shocked and angry but by dealing with it calmly your child will know they can turn to you again.

If you come across illegal content, such as images of child abuse, you can report this to the Internet Watch Foundation at www.iwf.org.uk in the UK, and find details of other national hotlines at www.inhope.org.

What are the ways this device can be used to communicate with others?

While they don't allow texting and calling in the same way as phones, these devices do provide a wide range of communication channels – instant messaging apps, social networking, video calling, chatting to other players in games and emailing to name a few. It is a good idea to chat to your child to understand how they use their device to communicate.

As these devices can be used to go online, many users will access social networking sites like Facebook. Safe social networking should be part of the conversation you have with your child, covering topics such as privacy settings, what's okay and not okay to post, as well as how to block and report. See our guide to social media.

Encourage your child to think about how they communicate; like other information posted online, content can be copied, edited or passed on to other people. Once it is sent you have lost control of it. Ensure that your child thinks about their responsibilities not to pass on information that might be hurtful or illegal.

The most popular apps with young people are games, and as part of their functionality, these offer an opportunity for communication. Many such games are for users to play alone, but many app games allow you to play against other players and make online friends that you don't know in real life, with integrated chat rooms so you can chat to other gamers while you play. For example, UNO for iPad and iPod Touch encourages you to "make new friends" over the internet. (See the app review from Common Sense). Playing such games can be fun, but it is important to ensure children know how to stay safe, by keeping personal information private and not agreeing to meet up with someone they have only met in this way. Talk to your child – are they chatting to strangers while they play games? Ensure that the content of the chat is appropriate and discuss what they should do if someone makes them feel uncomfortable. On some devices you can restrict the ability to take part in multiplayer games (see iPad, iPod Touch or Kindle Fire tips).

What to do about unwanted contact?

Ensure your child knows how to block contacts on Facebook or any other communication channels they use, and knows how to make reports to any service they use.

If you suspect that your child is or has been the subject of an inappropriate sexual contact or approach by another person you should report this to Child Exploitation and Online Protection Centre at www.ceop.police.uk in the UK, and internationally at www.virtualglobaltaskforce.com.

How is my child's location shared?

Location services allow applications such as maps and social networks to pinpoint your location. While it might be helpful to know where you are on a map to navigate your way home, it is important to be careful when sharing such information with other people. For example, Facebook allows users to update their status with their location. While this is turned off for younger users, it is worth noting that many young people do not register with the correct age and so need to choose not to disclose their location. Additionally, social networking apps like FourSquare, Google Latitude or Gowalla use the device's GPS to share location.

Speak to older children about the potential consequences of sharing their location and help them to think very carefully about what they share. With younger children you could have a family agreement about not sharing location at all, or perhaps you could use parental control tools to prevent them sharing their location at all (see iPad, iPod Touch or Kindle Fire tips for example).

What should I do if I think my child is spending too much time on their device?

Young people can often feel they need to be regularly communicating to keep up with their friendships - and with friends, games, music and films at their fingertips 24 hours a day it is easy to see how young people can become 'hooked' on their devices.

It is useful to have a family agreement about how your child uses their device, for example, agreeing rules about devices being switched off at night, or perhaps limiting the hours allowed on it as you might do for television. Remember that you need to model good behaviour, and if you decide that devices must be off at mealtimes, the same rules also need to apply to you! It is helpful for young people to understand that they are in control of when they reply to friends and that time away from their device is okay.