

About this guide

This guide has been produced to give parents information about Internet Safety. Much of the information comes from the CEOP - Child Exploitation and Online Protection Centre. Some of the information here is more relevant to those of you with older children but it is important to be aware of the potential dangers of using ICT at home.

Internet Safety tips

- Help your children to understand that they should never give out personal details to online friends they do not know offline.
- Explain to your children what information about them is personal: i.e. email address, mobile number, school name, sports club, arrangements for meeting up with friends and any pictures or videos of themselves, their family or friends. Small pieces of information can easily be pieced together to form a comprehensive insight into their lives and daily activities.
- Make your children aware that they need to think carefully about the information and pictures they post on their profiles. Inform them that once published online, anyone can change or share these images of them.
- It can be easy to forget that the internet is not a private space, and as a result sometimes young people engage in risky behaviour online. Advise your children not to post any pictures, videos or information on their profiles, or in chat rooms, that they would not want a parent or carer to see.
- If your child receives spam or junk email and texts, remind them never to believe their contents, reply to them or use them.
- It's not a good idea for your child to open files that are from people they don't know. They won't know what they contain—it could be a virus, or worse - an inappropriate image or film.
- Help your child to understand that some people lie online and that therefore it's better to keep online mates online. They should never agree to meet up with any strangers.
- Always keep communication open for a child to know that it's never too late to tell someone if something makes them feel uncomfortable. **Heronshaw School recommends the use of safer child based search engines such as:** <http://search.bbc.co.uk>, <http://kids.yahoo.com/> or <http://www.askkids.com/>
We also recommend the use of internet filtering software for home PCs. and that home PCs or games consoles with internet access are regularly checked and monitored by parents.



E-Safety

PARENTS

Social Networking

Social Networking websites utilise applications which help connect friends using a number of tools like blogs, profiles, internal email systems and photos. Well known sites include Bebo, Myspace, Facebook and Live Journal, and these have become an influential part of contemporary culture.

Firstly, the user signs up and creates their own profile or 'space'. Often, these contain standard sections such as 'About Me' and 'Who I'd Like to Meet' and also include things like Music, Films, Sports, 'Scared Of' and 'Happiest When'. They can also add specific personal details such as physical appearance, and the school they go to.

If they are talking to another child there is a risk that they will misuse this information - for example, by texting abusive messages to the child, or by posting their image on a website. Please be aware that some games consoles also enable children to send messages to each other and you should make yourself aware if your child can do this. There is also a risk that the person that they are chatting to is an adult. Unfortunately, undesirable adults use the internet, often with the intention of talking with and meeting a child. Young people can be naive to this risk, and often feel that they are invincible, or that 'they would know if someone was lying'.

- Encourage them only to upload pictures that you as their parents / carer would be happy to see. It's also not a good idea to post pictures which can identify the school which your child attends since this could help someone locate them.
- Tell your children not to post their phone number or email address on their homepage.
- Help your child to adjust their account settings so that only approved friends can instant message them. This won't ruin their social life - new people can still send them friend requests and message them.
- Check if your child has ticked the "no picture forwarding" option on their social networking site settings page - this will stop people sending pictures from their page around the world without their consent.
- Encourage them not to give too much away in a blog. Friends can call them for the address of the latest party rather than read about it on their site.
- Ask them to show you how to use a social networking site - getting involved will empower them to share the experience with you

NB Heronshaw School does not recommend the use of Social networking sites for primary age pupils.

Cyber Bullying

Cyber bullying is the use of ICT, particularly mobile phones and the internet, to deliberately to upset someone else.

Some simple ways to keep children safe online:

- Get to know your child's online habits. Children are inquisitive. They will look to explore the internet as much as they do the real world. Knowing the sites they go to, the people they meet there and what they do will help to keep children safe.
- Stay alert to any sudden changes in mood or appearance, or to any major change in habits or to increased secretiveness. These are often tell-tale signs that something is not right.
- Keep lines of communication open - tell your child they can always talk to you or another trusted adult, such as a teacher, if they do end up in some sort of trouble on the internet. Make children aware that there are things on the internet which may distress them.
- Spend some time surfing the internet yourself. The more that you know about the internet, the better able you are, in turn, to help your child navigate around it without coming to any harm.
- Install internet filtering software showing a Child Safety Online Kitemark on your computer. Filtering products with a Kitemark have been independently tested to provide a simple and effective means of support to parents, helping to ensure that a child's online experience is a safe one. The Kitemark scheme is sponsored by the Home Office and Ofcom.

Mobile Phones

There are some risks in their use of mobile technology. A large proportion of new mobile phones have web access, and more recently - mobile TV has been launched. This means that young people can access content from the internet and TV wherever they are, and without parental or teacher supervision. With the advent of picture and video messaging young people need to be increasingly careful about the images they share. It is very easy for inappropriate images to be shared around a number of phones, changed and even put online, where it is impossible to get back. Young people also need to be aware that they put themselves at risk of mobile bullying if they give out their mobile number to people they don't fully trust.

There are now mobile phone operators who sell phones with filtering software included so that children won't access inappropriate websites or content. It is worth checking that your child's phone has this capability. Remind your child that any image they send on their mobile can be changed and shared online, and that once they have sent an image they have lost control of it.



E-Safety

PARENTS

Instant Messaging and Chat

Instant messaging (IM) is a form of real-time text-based communication conveyed over a network, such as the internet, between two or more people on a user's contact list. Examples include Windows Live Messenger, Jabber, ICQ and AIM. IM technologies often include additional features that make them even more popular such as having the ability to talk directly for free; to share files; or to view the other party through a webcam.

A chat room is an online forum where people can chat online (talk by broadcasting messages to people on the same forum in real time). Sometimes these venues are moderated either by limiting who is allowed to speak (not common), or by having moderation volunteers patrol the venue watching for disruptive or otherwise undesirable behaviour.

Although chatting online can be great fun, young people can sometimes find themselves in situations where they can feel out of their depth. Risks can arise when young people give out their personal details to strangers. The online world can often seem very different to the real world for young people, and they can be tempted to say and do things that they wouldn't dream of if they met someone face to face. This can include giving out personal information such as mobile numbers and pictures of themselves. If they are talking to another child there is a risk that they will misuse this information—for example, by texting abusive messages to the child, or by posting their image on a website; but there is obviously a greater risk if the person that they are chatting to is an adult.

Young people can be naive to risks that technology poses. They will often 'swap friends' through IM, and therefore can be chatting to strangers who they feel they trust because a friend of a friend knows them. IM is a very intimate form of communication—more so than a chat room with many participants, and therefore adults will often use this as a means to extract personal information from a young person.

You can minimise the risks by taking the following simple measures with your children: It is vital that you know if your child uses chat applications online, and that you emphasise to them the importance of keeping their personal information personal.

- If your child uses IM then it is a good idea to ask them to show you how it works—in this way you can also gauge who they have on their contact list and if there is anyone how they don't know in the real world.
- It is also a good idea to ask them if they know how to block someone who they no longer wish to talk to.
- Consider creating some family rules which you will all agree to on online use, including not giving out personal information, or talking to strangers without discussing it.
- Remind your children that they should never meet up with someone that they have met online.

Gaming

Gaming sites can be fantastic fun for young people, however as with any online technology - there are risks:

***Addiction**

Online gaming can be addictive for young people. They can become so involved in the gaming communities that they lose touch with their offline friends in favour of spending time with online users playing games. Young people often spend hours every night playing games, especially when their parents have gone to bed. For this reason, CEOP recommends that the computer is kept in a family room. Parents will also then be able to monitor what games their children are playing, to ensure they are age appropriate.

***Abuse**

Some young people who use online games can be abusive to other gamers. This can range from saying nasty things if there is a chat facility within the gaming site, to always winning and not sharing cheats or knowledge on how to progress to the next level. Young people should be encouraged that when they play online games, they treat others how they would like to be treated. Be aware of any messages that your child sends and receives.

***Risky behaviour**

There are some young people who engage in risky behaviour to obtain cheats or knowledge to progress within a game and some people may try to encourage others to engage in inappropriate behaviour for rewards. Young people need to understand that their online behaviour has offline consequences and that if someone engages them in an unusual or inappropriate manner online they should inform a trusted adult immediately.

Playing games online can be a fantastic past-time for young people, but as parents you may not understand why your child spends so much time playing or how to help keep them safe. It's a good idea to keep the computer in a family room. This is so you can monitor the games your child is playing online, to ensure they are age appropriate and also so your child won't engage in activities that could put them at risk. This also means that children will not have the opportunity to spend hours playing games in the privacy of their bedroom after you have gone to bed!

As a parent, it's vital that you talk to your child and make sure they know how they should behave when they are gaming. They should be encouraged not to accept cheats or talk to people that they don't know in the real world. If anyone asks them to do anything that makes them feel uncomfortable, they should tell you or another trusted adult. It is a sensible precaution to monitor your child's use of any computers or games consoles in the house.

E-Mail

We do not use email for children at Heronshaw but you may have older children who do use it at home or at school. Email accounts are available from a huge range of different sources such as Microsoft, Google or Yahoo, but we do not recommend these to primary pupils because of the exposure to large quantities of unsavoury spam mail. If any of your children do use email, we would recommend that they should delete emails from people that they don't know. We encourage children not to tell anyone that they don't know any personal details.