Internet Security

'Internet Security' is the term used to describe the task of keeping children safe whilst they are online. Children and young people regularly use email, chat rooms, game websites and more; it is important that in doing so they are protected from people that would try to use these mediums to befriend, groom or abuse them. It is also important that children and young people are not able to access, or be exposed to, images or content that is deemed inappropriate by law for their age.

The internet opens up a world of entertainment, opportunity and knowledge. To help your child to enjoy it all safely, the UK Council for Child Internet Safety [UKCCIS] has developed the 'Click Clever, Click Safe' code.

'Zip it, Block it, Flag it': a guide to the code

The code has been designed to:

- give parents the confidence to be able to help their children enjoy the internet safely
- help children and young people understand how their online experiences can expose them to risks

The code has three simple actions:

- **Zip it**: keep your personal information private and think about what you say and do online
- **Block it**: block people who send you unpleasant messages and don't open unknown links and attachments
- **Flag it**: flag up with someone you trust if anything upsets you or if someone asks to meet you offline

It's easy to remember when talking to children about online safety and it's designed to help keep them safe on the internet.

Zip it

Make sure your child knows to always keep private information safe and watch what they say on the internet. People may not be who they say they are online and it's not always possible to control who can see your child's information.
Your child should know not to give out information like:

- their full name
- photos
- postal or email addresses
- school information
- mobile or home telephone numbers
- details of places they like to spend time

Make sure your child knows that they shouldn't arrange to meet people that they have only met online. Even if they have been chatting with someone for a while, that person is still a stranger.
You can help keep your child's information safe by setting privacy settings. This can restrict access to personal information and photos on things like social networking sites.

You should also encourage your child to use a nickname instead of their real name in chat rooms or on instant messaging services. To stop people accessing your child's online accounts, encourage them to keep their passwords secret, and to change them regularly.

Block it

Get your child to block people who send offensive messages and tell them not to open unknown links and attachments. They should delete any suspicious emails or attachments as they may contain something offensive or have a virus that can cause damage to the computer.
One of the main ways children can come across inappropriate content online is through search results. Most search engines include a 'safe search' option that excludes results containing inappropriate images or key words.
You can also install parental control software to filter out harmful and inappropriate content for computers and some mobile phones and games consoles.

Flag it

The final rule is that your child should come to you or a trusted adult if they are worried or unhappy about anything they see online. They should also do this if a friend they have made online has asked to meet them in the offline world.
If your child does experience inappropriate content online, report it to the website it appears on. UKCCIS has developed an internet safety 'one stop shop' with more information.

Cyberbullying: talk to your child about staying safe on computers and mobile phones

These days bullying doesn't just happen in the playground. Cyberbullying, or bullying via digital technologies like mobile phones and computers, is a different threat to your child. It can be harder to spot and more difficult to manage than 'traditional' bullying. Understanding the dangers will help you support your child.

What makes cyberbullying different

As with other forms of bullying, usually the bully intends to cause harm and carries out activity over a period of time. Cyberbullying is different to other forms of bullying because:

- it can occur at any time of day, anywhere; the victim can even receive bullying messages or materials at home
- the audience to the bullying can be large and reached very quickly and easily if messages are passed around or things are posted online
- it can be unintentional; because they are not face to face, people may not think about the consequences of sending messages or images

Ways of cybrerbullying

Some of the ways of cyberbullying can occur are through:

- chat rooms, blogs and forums: although some of these are moderated, people involved in discussions can be sent abusive responses
- text messaging: abusive and threatening texts can be sent to mobile phones
- abusive or prank phone calls: these can be made to your child's mobile phone

- picture and video clip messaging: offensive images can be sent to mobile phones
- email: new addresses can be set up in minutes and used to send offensive messages and images
- social networking and personal websites [like Facebook or MySpace]: offensive or humiliating messages and images can be posted on these sites
- identity theft: in many online environments fake profiles can be set up pretending to be someone else with the aim of bullying others instant message services; quicker than email, these allow users to have 'real time' conversations, and offensive messages or content can be sent in this way
- webcams: usually used to view each other when chatting online, children can also be sent abusive images or encouraged to act in an inappropriate way while being filmed
- video hosting sites (like YouTube): children may find themselves the subject of films being shown or be accidentally exposed to pornographic images
- gaming sites, consoles and virtual worlds: chatting is possible within many games, and name calling, abusive remarks and picking on particular players can occur

Minimising the risks of cyberbullying

As with other types of bullying it's important for you to listen to your child and react with sympathy. Your child should know that bullying is always wrong and that seeking help is the right thing to do. It's important for them to learn to respect and look after their friends online just as they would face to face. You should talk to your children about who they are talking to online. Try to guide them by discussing sensitively the issues around online friends. Negotiate and establish boundaries. You should also make sure you:

- are aware that there are many ways children can go 'online', such as on a mobile phone or games console
- encourage your children to talk to you or another adult about anything that's upsetting them
- watch out for them seeming upset after using a computer or their mobile phone
- try to understand the ways in which they are using their digital technologies
- ask them to think about how their actions affect other users
- suggest that they avoid private chat rooms
- encourage them to keep evidence of any abusive or offensive emails or messages they've received, and to show you or another trusted adult
- help them report any abuse to their school, the internet service provider, the website manager/moderator, the mobile phone company or the police
- tell them not to respond to any abusive messages or calls; this is frequently what the abuser wants
- discuss keeping their passwords safe and avoiding giving personal information, such as their name or mobile phone number to people they do not know face to face
- change email address or telephone number if the abuse continues
- turn on in-built internet safety features and install computer software to ensure that you only receive emails from people you have chosen and to block unwanted images
- tell them about places where they can go for help and support like CyberMentors, ChildLine and Childnet International

Where your child will chat / communicate

The internet lets users chat with friends and family in interactive 'virtual' communities. These communities are increasingly popular with children because they allow them to communicate in 'real time'.
'Real time' means their contributions [or 'posts'] are displayed immediately, for example in online chat or via messenger services. However, not all virtual communities will be moderated or supervised. The following are examples of sites your child may use to chat with others online:

- chat rooms are 'virtual' rooms where users can 'talk' with each other by typing, either one-on-one or involving a number of people
- forums are online discussion groups - these discussions can take place in real time or over a longer period [users can continue to add comments]
- instant messaging services [which look like small pop-up windows] let users see when people on their 'friends list' are online and send messages to them
- social networking sites are online communities of people; users have a number of different ways of communicating with each other

Online dangers to be aware of:

Grooming

Offenders pretend to be children themselves to start online conversations
The internet can be fun and useful but you and your child need to know the risks too. Making sure your child knows the online dangers is just as important as teaching them to cross the road safely.

Grooming

Unfortunately, some adults with a sexual interest in children will use the internet to communicate with them. Online grooming is when a suspected paedophile behaves in a way that suggests they are trying to contact children for illegal purposes.
You should talk to your children about who they are talking to online. Try to guide their online behaviour by negotiating and establishing boundaries. Discuss the issue of online friends sensitively. If they have not met someone face to face, they could be anyone.
It may be possible to use parental controls to block access to some online services altogether.
Sometimes offenders pretend to be children themselves, to start online conversations with real children. They might then try to continue the relationship in personal conversations on mobile phones [sometimes known as 'whispering']. This can be very convincing and children might think they know someone as a result of this intimate contact.
Once they have established some trust, the offender may try to organise a meeting with the child. This may take weeks, months or even years.
As part of the grooming process, the offender might also try to exploit them by sending them indecent or pornographic images. This might be by email or sometimes by using a webcam [a camera connected to a computer, which can produce still pictures and video footage].
The offender may even use blackmail to persuade the child to do something they don't want to. It is vital your child knows that not everyone on the internet is who they claim to be. It's also important both you and your child report anything suspicious.

Cyberbullying and cyberstalking

Cyberbullying is bullying online, for example through using computers and mobile phones. If someone is stalking someone else over the internet it's known as cyberstalking.

Reporting suspected grooming or cyberbullying

You and your child can report any suspicious, threatening or offensive behaviour to the Child Exploitation and Online Protection (CEOP) centre.

Protecting your child online

It is impossible to be completely protected while using the internet. However, you can take simple steps to reduce the risks.
You should always set the parental controls to any device that connects to the internet. Access to the internet could be via a computer, mobile phone or games console. These are easily set up and you can check the equipment's user manual or the manufacturer's website to see what controls you have access to. The controls will let you block troublesome email senders or access to certain websites.
Device-level parental controls means you set up settings for each individual user. This means you are able to restrict access to certain online services, or networks for each individual user.

Social networking sites

Social networking sites (like Facebook, MySpace or Bebo) are online 'communities' of internet users with similar interests. Members of the community create an online 'profile' which provides other users with varying amounts of personal information.
Once users have joined the network, they can communicate with each other and share things like music, photos and films. The sites are a fun way for your child to stay connected with their friends, family and peers.

What are the potential dangers?

Social networking sites are seen as being very 'cool' by children and they may be pressured by their friends into joining them. The sites don't actually present any threats that don't already exist elsewhere online. The danger is that the threats exist in a new online environment you or your child may not be familiar with.
As with most potential online dangers, the problems can start if your child doesn't look after their personal information properly. The risks you need to be aware of are:

- cyberbullying (bullying using digital technology)
- invasion of privacy
- identity theft
- your child seeing offensive images and messages
- the presence of strangers who may be there to 'groom' other members

Registering and using safe settings

If your child's about to join a networking site, there are things you can do to improve their security before they even start using it.

Privacy settings

Get your child to select the strongest privacy setting available when they create their account. This will ensure that their personal information is only seen by people they want to share it with. However, be aware that some sites are totally open to the public.

Safety tools

Learn about and make sure your child knows about the safety tools available to them on the service they're using. This might include a block function to stop unwanted contact or the option of pre-approving comments posted onto their profile before they are made public.

Profile/screen name

Although your child may be able to limit who has access to their profile, their profile/screen name shouldn't include their real name.

Staying safe while using social networking sites

The following guidelines will help make sure your child is safe while they are members of social networking sites:

- make sure that they don't publish personal information like their location, email address, phone number or date of birth
- make sure your child is very careful about what images and messages they post, even among trusted friends; once they are online they can be shared widely and are extremely difficult to get removed
- encourage them to talk to you if they come across anything they find offensive or upsetting
- keep a record of anything abusive or offensive they've received and report any trouble to the site management [most sites have a simple reporting procedure, normally activated by clicking on a link on the page]
- make sure they're aware that publishing or sharing anything which would mean breaking a copyright agreement is illegal
- if your child makes an online friend and wants to meet up with them in real life, you should go along with them to check the person is who they say they are
- tell them to be aware of online scams; offers which seem too good to be true usually are
- encourage them not to get into any online discussions about sex as these tend to attract potentially dangerous users
- if you suspect someone may be grooming your child on a social networking site, or your child is being stalked or harassed, you should contact the local police or Child Exploitation and Online Protection Centre [CEOP]

How children chat online

- It's also helpful to learn how your child communicates online. Children often use shortened versions of words or acronyms of phrases - for example 'LOL' for 'laughing out loud'.
- It's very common for people to do this when using message boards and social networking sites. You can find out what any of these acronyms mean by searching for them online.