what parents need to know

The guide to safe and responsible use of mobile phones and the Internet

orange™

introduction

This guide offers advice on how you and your family can safely get the best out of mobile phones and the Internet. Technology continues to develop rapidly and our children are now growing up with all sorts of gadgets and gizmos as the norm. And, although it doesn't seem complicated or scary to them, it's often a different matter for parents who can feel left behind and out of touch.

The challenge for everyone, but particularly parents, is to make sure children fully understand and are prepared for the possibilities, both good and bad, presented by new technology.

We hope you find this guide useful and we have tried to include as much information as possible without overloading you. You can read more about mobile phone and Internet safety by visiting our website at orange.co.uk/safety

contents

mobile phones

In only ten years, mobiles have evolved from a mobile version of the traditional phone into something closer to a handheld personal computer, TV, video camera and music system.

Although mobiles have brought with them many benefits, there are ways of using them that are antisocial or undesirable. These vary from people having loud mobile conversations on public transport – to 'spam' text messages or harassment.

Access to the Internet on mobiles has also made available types of material that are unsuitable for children and that many adults may not want to be exposed to either. And – because they are small and desirable – mobiles are often the target of thieves.

before using a mobile phone for the first time

- agree with your children how you want the phone to be used. Talk about the use of paid-for services (like music and video clips – or time spent on the Internet) so you can avoid nasty surprises with the first bill
- try and discuss adult-content issues in a way that lets children feel able to bring up the topic again if they need to. Although we provide Safeguard to block access to adult material on mobiles, that doesn't mean that their friends use phones or computers on which this is effectively blocked
- you will probably need to have more than one conversation on mobile phone safety as your child develops and new services emerge all the time
- it is a good idea to share experiences about modern technology with other parents. Doing so may help shed useful light on issues before they become a problem for you or your children

bullying and harassment by mobile

Familiarity with mobile technology has enabled some children to develop ways of using mobiles to intimidate and harass others.

For instance they may:

- leave threatening voice messages
- send threatening text messages
- distribute images taken with phone cameras

Intimidation by phone may be part of a wider pattern of bullying but it can be all the more unpleasant because it reaches into the home.

If bullying from school mates is suspected it is vital that you report it to the school as soon as you can.

Talking points and advice

Before your children take their mobiles out and about, give them the following advice:

- never give out any information about yourself unless you know the caller
- let the caller identify themselves – particularly if no number is displayed
- if you receive a call from a problem number, don't respond: divert such calls to your mailbox without answering
- do not leave alternative contact details on your mailbox greeting
- be very careful who you give your number to and ask those you have given it to not to pass it on
- turn off the Bluetooth® function on your phone if this is how unwanted messages are being received

If they do receive a nuisance text they should:

- never respond to the message
- show it to a trusted family member, teacher or parent
- keep the message as evidence

- make a note of the sender's number or the originating details they'll find at the end of the message

Things we can do if you call customer services:

- arrange for the phone number to be changed
- if you wish, our dedicated Malicious Calls Bureau can supply relevant information to the police. Due to Data Protection law we cannot supply caller information directly to you

Harassment and bullying by mobile phone can be dealt with as an offence under Section 127 of the Communications Act 2003, regarding the improper use of public electronic communications networks.

We can't currently block numbers through our network but some types of phones can do this so check your manufacturer's guide.

More information

The following sites contain information on the subject of bullying in general:

bullying.co.uk

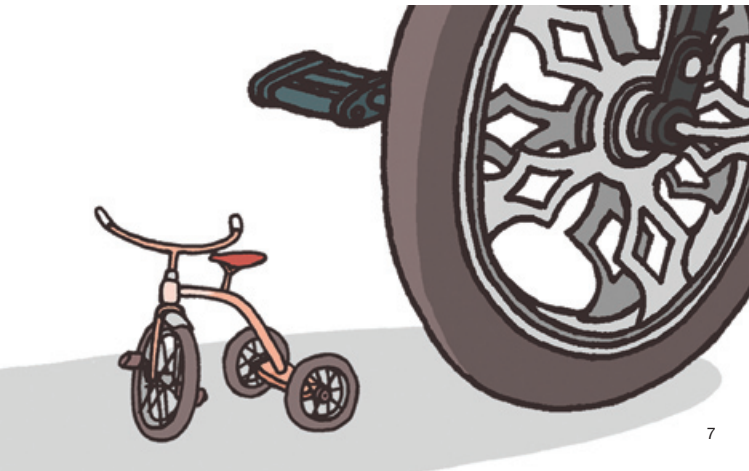
kidscape.org.uk

besomeonetotell.org.uk

And these have information on bullying and text messages:

stopcyberbullying.org

dcsf.gov.uk/bullying/

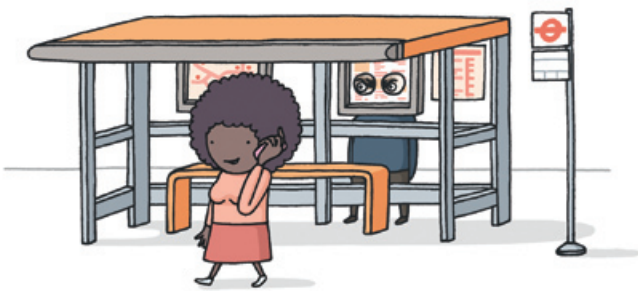


misuse of emergency services – hoax emergency calls

Far from being a ‘prank’, these calls actually put other people’s lives at risk and these waste the emergency services’ resources.

Talking points and advice

- point out the danger and irresponsibility of hoax 999 calls before use
- point out that such behaviour has consequences for your child as well as those they endanger. Making false 999 or 112 calls is a criminal offence and can result in an application by the emergency services to have the offending phone terminated from the network. Emergency services can also request subscriber details, which may lead to criminal proceedings. Both actions are now being taken more frequently by the emergency services
- care should also be taken when handsets are in bags or pockets. They are designed to allow 999 calls even with the keypad locked



phone theft and street safety

As mobile phone ownership has increased, phones have gradually become 'fashion accessories' – especially for young people. This has increased their attractiveness to thieves.

Advice

For children and young people, the greatest threat of theft comes from other young people. The best ways to reduce the risk are:

- avoid showing a new phone around – except to close and trusted friends
- avoid making calls in very visible and public places – make them discreetly. A high proportion of phone thefts take place when the victim is making a call
- avoid being overheard – especially if arranging a meeting

What can you do if your phone is stolen?

- call customer services immediately so that we can bar the SIM card*, block calls from the phone account and immobilise the phone using the IMEI number**. This will stop your handset from being used on all UK mobile networks

Remember to register your IMEI number, free of charge and online, by visiting **immobilise.com**. This service also allows police to identify the original owner of recovered phones. Immobilise is not just a mobile phone register it is a national property register.

* A SIM card (Subscriber Identity Module) is the removable chip inside a mobile phone with information such as the user's phone number, phone book as well as other information related to the subscriber.

** An IMEI number is a unique identifier for a particular handset and can be found by pressing *#06# on the keypad.

Music players

Many mobile phones now feature built-in music players – a source of appeal to children and teens, so its important that you remind them to be extra careful crossing roads, or using bicycles or scooters, while listening to music.

Advice

- do not bicycle or use a scooter with music playing so loudly that you can't hear other traffic
- be extra careful if crossing roads while listening to music, speaking on the phone or texting

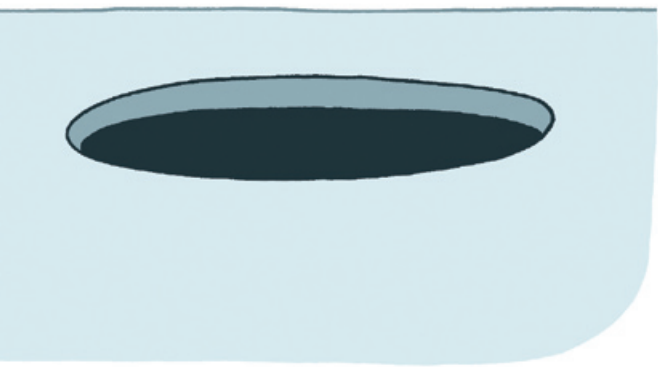
Street safety is not all about children, so while we have your undivided attention we have some advice for parents too on the subject of driving and the use of mobiles.

Unless you have a hands-free kit, it is an offence to use a mobile in any way while driving and you can be fined for doing so even if the car is in stationary traffic. If you were involved in an accident the police can now bring criminal charges if dangerous driving was involved so its important that you use a hands-free kit.

If you don't have a handsfree kit you should pull over, stop in a safe place, and turn the engine off before making or taking a call. Even if you do have a hands-free kit, it is still safer to pull over before making or taking a call. It is highly dangerous to write or read text messages while driving.

Advice

- never use a mobile without a handsfree kit while driving
- even if you're using a hands-free device it is safer to tell the caller that you're driving and will call them back later (when your journey has finished or when you've pulled off the road, with the vehicle stopped and its engine turned off)



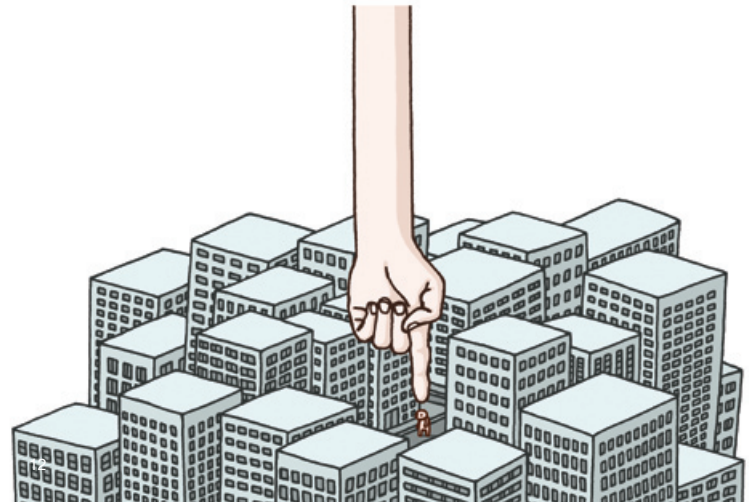
location-based services

What are they?

Location-based services (LBS) are services that depend on a service provider knowing where a mobile phone user happens to be. Services that rely on the mobile network knowing where a phone is are covered by the location industry code of practice, developed in 2004. New services hitting the market make use of GPS technology inside some mobile phones to pinpoint a user and provide them with for example maps or directions to a restaurant. Some can even work if you don't have GPS but the location is less accurate. The services require a user to sign up or accept Terms and Conditions when they download the application.

For more details go to:

orange.co.uk/documents/regulatory_affairs/ls_cop_locationservices_outline_240904.pdf



But there are concerns:

- unwitting use. It is possible that 'spam'-type messages could trick people into signing up for location-based services without fully understanding the implications
- security of children. A concern is that if third parties were able to persuade the end-user of a mobile phone to consent to tracking, the use of this information could put children at risk

Talking points and advice

- your children should understand why they should never say 'yes' to a stranger or someone they don't trust who is trying to find them through a location based service
- discuss with your child who their friends are on social networking sites and explain why it may not be wise to allow all these 'friends' to share their location information. Use privacy settings to restrict location information to only close friends or family
- explain that they should ask you before accepting any kind of service offered over the phone and, if they are not sure, it is always best to check
- if you suspect that an LBS is being used inappropriately call Orange customer services

spam and unsolicited messages

What is it?

'Spam' is an unwanted marketing message that you have not actively asked for or subscribed to. Things like 'you have won a 'mystery prize' or asking you to call a premium-rate number.

It's just another version of 'junk mail' or the phone sales calls you get at home.

How do 'spam' messages work?

Sometimes the phone numbers are randomly generated. Lists of phone numbers can also be illegitimately compiled and sold on to companies as 'marketing lists'. In these cases, the same text is sent to thousands of customers, so you or your child won't have been singled out.

The problem affects all mobile networks, and Orange itself does not provide customer telephone numbers to other companies for marketing purposes.

Talking points and advice

- explain the risks of replying to spam messages or calling the number in the message – this may be charged at a premium rate
- encourage your child to ask you before accepting offers on their phone

Ending services

- if details about cancelling a service are not contained in the message, a search on the web, or through directory enquiries, will usually give the sender's contact information. Contact the sender directly to remove your number from their marketing list
- if you are receiving text messages from a short code number for a service that you subscribed to but no longer wish to receive, try checking their instructions. Typically the way to deregister is to text the word 'STOP' to the service. If you do not have their details, call Orange customer services, which may be able to assist with contact details for the service provider

How to avoid spam

- read terms and conditions on forms carefully before giving out your mobile number
- you should tick or untick permission boxes when filling in online or paper forms
- never sign up with websites that promise to remove your name from spam lists. Some may be legitimate, but others actually collect mobile phone numbers

Send your spam to us

If you receive spam messages, please forward them to 7726 free from your Orange phone. By doing this you are helping Orange collate information that may help reduce the volume of spam messages being sent to you and others.

Notify the watchdog

Suspected premium-rate SMS scams should be reported to PhonepayPlus – the organisation that regulates products or services. You can contact PhonepayPlus by dialling 020 7940 7474 or by visiting **phonepayplus.org.uk**

Telephone Preference Service

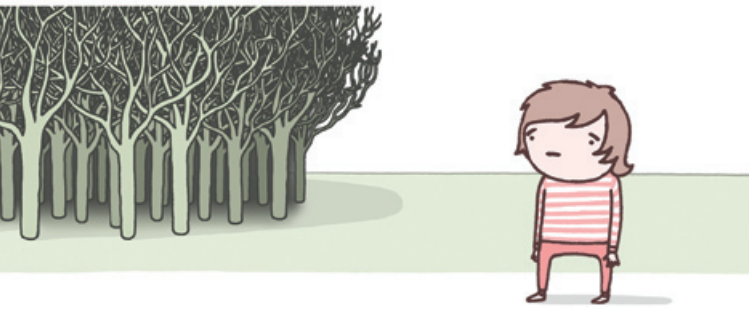
You can also register – for free – with the Telephone Preference Service to stop commercial calls being made to your number. For more details visit: **tpsonline.org.uk/**

adult content and the Internet

What is ‘adult content’?

Modern phones – and especially those that allow access to the Internet – offer a range of services and information intended for adults.

In this sense, mobile phones are becoming more like computers and are used as a doorway or ‘portal’ to a wide range of content and services. Not all of this is suitable for children or even some adults. In particular, there are sites containing pornography, violence and gambling that many parents will find unwelcome.



Talking points and advice

Does the phone I’ve bought give access to the Internet?

These days the answer is probably yes – and definitely so if the phone is either ‘3G’ or ‘WAP enabled’. See the phone jargon section at the end of this guide.

Can I block adult material?

Orange offers a service called ‘Safeguard’ which is a filtering service covering Internet content. Orange Safeguard is designed to prevent anyone under the age of 18 from reaching adult content, while enabling them to surf the rest of the Internet. The filtering service follows the Independent Mobile Classification Body (imcb.org.uk) guidelines.

Does my phone have the filter?

The Orange Safeguard filter is automatically applied to all new 'pay as you go' accounts. Orange Safeguard is not applied automatically to 'pay monthly' or contract customer accounts as anyone with such an account is assumed to be over 18, having been through a credit reference process at the time of purchase.

However, if a parent or guardian has provided a contract phone to someone under 18 – or a phone is being passed down from another member of the family – they can contact Orange customer services to request that Safeguard be applied to that phone account.

Pay as you go customers who are aged 18 or over and want to receive adult content can verify they're over 18 in one of three ways:

- by making a credit card transaction via customer services. This can take the form of a pay as you go top-up paid for by credit card (debit cards are not allowed for age-verification)
- by customer services making a third-party credit bureau age check
- by taking physical ID – such as a passport – to an Orange shop

For further information please go to help.orange.co.uk and search for 'blocking adult content'.

Important note: remember that if you have bought a monthly contract phone for your child, the Safeguard filter won't automatically be switched on – tell us as soon as you can that the user is under 18 and we can apply Safeguard. If you are not an Orange customer its best to contact your phone provider and check what settings have been applied.

picture and video messaging

Taking, storing and sending pictures taken with camera phones is a significant part of their attraction – especially for children.

However, safe and considerate use of these cameras requires a mix of care and common sense.

Talking points

- never send pictures that embarrass other people or show them partially clothed: this is especially true of images taken of other children. It is best to treat others as you would like them to treat you
- posting photos of yourself online in public areas could help you be identified by strangers
- sending unpleasant or indecent images to others may be an offence in certain situations
- everyone should obey any restrictions on the use of camera phones in places like swimming pools, schools and some gyms
- watch out for people – particularly unknown adults – taking pictures of you or your friends
- hitting other people for the purposes of recording the image on a camera phone (sometimes described as 'happy slapping') is an assault – and therefore a criminal offence. To watch it and laugh at it is a form of bullying even if you are not involved in the act. These images should never be passed on
- if you are sent an image of an assault on another individual, keep the image and show it straightaway to a parent, teacher or other trusted adult

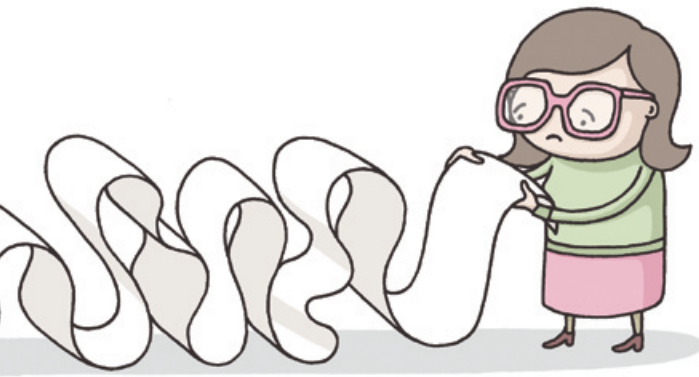
managing bills

Mobile phone tariffs can be complicated at the best of times and the last thing you need is a nasty surprise lurking in your monthly statement.

More and more, purchases can be made over mobiles, from simple ringtones and wallpaper (a picture for your home screen) to games and lottery tickets. Many of today's TV reality shows also allow you to text in your vote which can have a high cost.

- be careful to check what services are premium rate numbers
- talk to your children and agree in advance what extras they can buy
- read the small print – some services that require you to text in a word or code will often charge you for the reply message as well. Similarly some even have a monthly charge that can catch you out
- contact customer services if you want to bar international calls or calls to premium rate numbers
- remember, if a phone is stolen, you're liable for the cost of all calls until it's reported stolen, so you should report it as soon as possible. Refer to page 9 for information on phone theft

Premium Rate Services (PRS) are expensive and if you would like to read more about the Code of Practice that's in place visit our website at **orange.co.uk/safety** and go to the unexpected costs section.



mobile phones and health

Mobile phones are small two-way radios. They are only the latest development in a family of devices whose origins date back to the middle years of the last century.

Most mobile phones work in the microwave area of the radio spectrum. This region is also used by some TV transmitters, baby monitors, radar, wireless CCTV, Global Positioning Systems, 'wifi hotspots', police speed traps, garage door controls and car central-locking systems.

Research

Despite an extensive record of research going back several decades, the current position remains that there are, "No known health effects below [existing emission] limits" (World Health Organisation presentation, 2004). This view has been reinforced by numerous independent health science reviews carried out around the world in the last few years.

On the other hand, no previous wireless device has ever been used by millions of people on every continent. Because of this popularity, research continues in order to ensure that there are no small – and so far undiscovered – effects on small, possibly distinct groups within the wider population.

In July 2005 WHO gave a statement regarding EMF. "To date, all expert reviews on the health effects of exposure to RF [radio frequency] fields have reached the same conclusion: There have been no adverse health consequences established from exposure to RF fields at levels below the international guidelines on exposure limits published by the International Commission on Non-Ionizing Radiation Protection (ICNIRP).

The ICNIRP guidelines were developed to limit human exposure to electromagnetic fields (EMF) under conditions of maximum absorption of the fields, which rarely occurs, and the limits incorporate large safety factors to protect workers and even larger safety factors to protect the general public, including children. Thus, the limits in the ICNIRP guidelines are highly protective and are based on all the available scientific evidence."

who.int/peh-emf/meetings/ottawa_june05/en/index4.html

What protections are there?

All phones sold in Europe must comply with the emission standards compiled by the International Committee on Non-Ionising Radiation Protection (ICNIRP).

Importantly, the ICNIRP guidelines are designed not only to exclude all risk of known adverse health effects, but also to minimise the risk of any potential – but undiscovered – health effects. All Orange equipment complies with these guidelines.

More information

There is a lot of information about radio waves and mobile phone networks at the Orange site: **orange.co.uk/about/phone_masts/index.html**

Other useful sites include:

Health Protection Agency:

hpa.org.uk/radiation/understand/radiation_topics/emf/index.htm

UK Department of Health:

dh.gov.uk/Home/fs/en (Type 'mobile phone' into the site search engine.)

International Commission on Non-Ionising Radiation Protection:

News of research and other material can be found in the activities section at: **icnirp.de/index.html**

World Health Organisation:

Provides detailed and extensive information on electromagnetic fields and mobile phones at: **who.int/topics/radiation_non_ionizing/en/**

internet

Our kids are growing up with the Internet as part of their everyday life. This can often mean they're not as cautious as those of us that have seen it evolve in the last 10 years or so. Its become a part of the fabric of our life and a resource that we wonder how we ever lived without. The opportunities for communication, self expression and exploration are developing every day and while the Internet can provide exciting opportunities, it also creates a need for people to safeguard themselves and understand the need for care, restraint and responsibility.

Acceptable behaviour

Just as we know how to behave in everyday situations, either at home, the supermarket or school, there are boundaries of acceptable behaviour that also apply to the Internet. It's about respect, tolerance and privacy – many of the things we teach our children about already. It's no more acceptable to abuse people on social networking sites or share videos of people without their permission online than it is in the offline world.

Laws and regulation

There are a number of laws that cover behaviour on the Internet and as a general rule of thumb, if it's illegal offline, chances are it's illegal online too. These laws include (but are not limited to):

- Protection from Harassment Act (1997) – covers any form of persistent conduct which causes another alarm or distress
- Protection of Children Act (1978) – prohibits the creation and distribution of indecent photographs of children
- Sexual Offences Act (2003) – causing or inciting a child to engage in sexual activity, causing children to watch sexual acts and meeting a child following sexual 'grooming'
- Communications Act (2003) – covers the sending of offensive, indecent and obscene materials over the electronic communications network

You can find out more about these laws and how to go about reporting abuse online at **orange.co.uk/safety**

Anonymity

There is a common misconception that people are anonymous while on the web and this can lead to uncharacteristic or inappropriate behaviour. While other Internet users may not be able to tell who someone really is, service providers can identify users and if necessary may provide information, under appropriate legislation, to the police to help them find a criminal. Make sure children are aware all Internet users are responsible for their behaviour online and tell them they should report anything which makes them feel uncomfortable to you or a trusted adult.

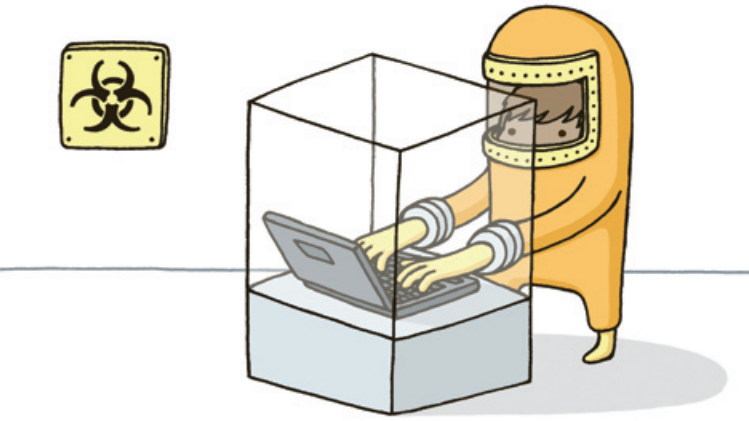
illegal and inappropriate content

Adult content, violence and self harm

There are many websites that are not suitable for under 18's and there is a difference between what is deemed illegal and what is 'inappropriate'. Orange work with the Internet Watch Foundation (IWF) to block access to illegal child abuse images and it's up to parents to restrict access to what you think may be unsuitable for your children.

Recently there has been a growth in websites that appear to promote things like anorexia, self harm and suicide as well as more extreme ones linked to crime and violence. Whilst some of these websites are not illegal, in law there is some balance needed between self expression, free speech and content that's considered dangerous The next section will provide information and advice that will help you filter web content effectively and tell you where to go for help if you need it.

For advice on matters like these you can contact various support services for confidential support and advice; we've listed some at the end of this booklet.



How can I protect my children online?

Make sure you have content filters or parental controls in place. This will block access to over 18 websites and you can have different profiles to allow other people in your household to access those sites if they wish. You can also use the filters to make sure younger children don't access social networking sites where age limits are typically 13 and over.

Orange Broadband customers can download parental controls filtering software for free from **orange.co.uk/communicate/security/**

Remember that websites that require you to be over 18 aren't illegal, and contrary to belief, they are not all based around pornography. There are things like gambling sites, as well as dating websites. Its up to you as a parent to make sure you have the right filters in place as these sites won't automatically be blocked.

Advice

Consider the benefits of having the home computer in a family area rather than your child's bedroom. Think about the portability of laptop computers and how children can take these anywhere they like so it's even more important to ensure you have thought about parental control software.

Online chat rooms

Chatrooms are websites where people exchange messages with people from all over the world – it's a type of open forum on the Internet. There are thousands of these sites catering for every imaginable hobby or interest and it's often a friendly and unthreatening place that children can visit and share experiences and information.

How can my children stay safe in a chatroom?

You can use filters to prevent access or other technology that monitors their conversations but the best thing you can do to help make your children safe online is to teach them about Internet safety. Talk to your children about the following things:

- be careful who you trust – people are not always who they say they are
- don't give out personal information about where you live/go to school/socialise etc
- use a nickname that doesn't give away your identity
- stay in charge – if the chat gets out of hand you have the control to stop it
- think before answering – especially if you are in a private chat room rather than a public one
- never meet up with anyone met through a chatroom unless accompanied by an adult
- don't open website links that are posted in chatrooms as these can contain viruses

Unfortunately the online world can also be used by those who use any opportunities to engage with children as a way to form relationships and gain their trust in a process known as 'grooming'.

There are a number of ways these abusers gain trust and if you suspect that this is happening to your child, you can find out more information about what signs to look for and how to deal with it through a dedicated law enforcement agency called CEOP (Child Exploitation Online Protection Centre): ceop.gov.uk

CEOP have a section on their website dedicated to parents where you can get advice and information if you believe that this may be happening to your child.

The important thing is to make sure that children are able to recognise the dangers and sense when something might be wrong. Remember online chat is not bad in itself and talking to strangers in chatrooms doesn't automatically mean someone is taking advantage.

So don't panic! Talk to your kids about who they chat to – you'll have to trust them to a certain extent and

as long as they know what to look for, they should be able to have healthy online conversations without putting themselves in any personal danger.

Cyberbullying

We know that children can be bullied by text message (see page 6) but bullying can also occur though instant messenger and social networking sites.

The most common forms are:

- posting abusive or threatening comments on someone's website, profile or blog
- posting pictures or videos of bullying incidents
- stealing passwords to post comments as the user and impersonating them in order to set up fake websites that are offensive
- excluding the victim from friends' groups

Bullying is not new, but the web has given bullies a new tool to intimidate their victims with, and bullies often believe, falsely, that they are anonymous. (See anonymity on page 23.)

More information:

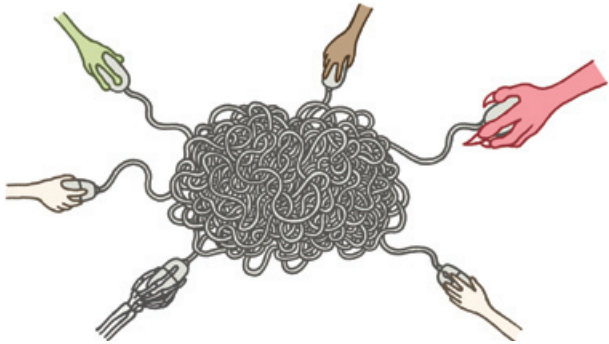
thinkuknow.co.uk/

digizen.org/cyberbullying/

social networking

The last couple of years have seen a rapid expansion in the number of websites that allow users to publish their own home page or 'profile'. They are popular with children and young people both as a means of self-expression and as a way to forge links with friends – an activity some call 'online social networking'.

The growth of these sites has been a phenomenon. For example, since Facebook launched in 2004 it has accumulated over 130 million worldwide users, it is the 4th most trafficked website in the world and is the No1 photo sharing site. You may have heard your children talk about Bebo, MySpace and Flickr which are also popular social networking sites.



Social networking sites are typically used as a place to post on-line diaries in the form of 'blogs'. They will often also contain pictures; lists of likes and dislikes; contact details; links to other content and more or less anything else the user feels like showing. Most sites also have the ability to leave messages.

To make the experience more appealing still, some sites offer software to allow users to decorate their own page with free graphics and artwork.

The latest social network site is Twitter which allows you to update a short text based profile so that people can follow what you are up to and get an insight into the lives of others. The process of updating the profile is called 'tweeting' and many celebrities and even political parties are Twittering these days. Anyone can sign up to 'follow' you if you have a public profile (although you can block followers) ; it's important that children only allow people they know to follow them.

Should I worry?

Websites of this sort usually have clear guidelines that users are asked to read before they sign up. These can include 'house rules' on user-age and advice on what not to 'post' – as well as a means of reporting undesirable or illegal content. Some also have dedicated teams of people to 'take down' inappropriate postings.

Posting personal information

Despite the fact that these sites can be fun and are mostly used for genuine socialising, some concerns remain. They include:

- **Privacy**

  Most social networking sites include privacy settings which can be used to control who can view content they post on their profile and in their blogs. Teenagers – a large proportion of users of these sites – don't always grasp that if their settings are public it can be seen by anyone in the world. Particular care should be taken when uploading photos as background detail can give away where people live or go to school.

- **Unwelcome visitors**

  As a magnet for teens, such sites are also popular with all sorts of people that parents would prefer their children did not encounter. These include: paedophiles, recruiters for extremist groups and those promoting dysfunctional conditions like self-harm, suicide obsession or eating disorders.

What can I do?

- familiarise yourself with how these sites operate and then reach an understanding with your child that you will periodically review what they post on their profiles. If this seems slightly invasive, ask yourself how comfortable you would feel letting your child contribute to the local paper or TV station without your oversight?
- use any obvious mistakes as an opportunity for both you and your child to learn – rather than overreact. These websites are not going away and you and your child will have to cope with the complexities of online activity for the rest of your lives

- regularly discuss your child's online activities in a way that encourages them to be open. It is generally easier for a child to cover their tracks than it is for parents to uncover them. An open and honest dialogue will help reduce the need to worry

Talking Points

- remember that anyone, anywhere, can see what you have posted. So be careful what you say: it may affect more than you think. In America, some college recruiters and potential employers have taken to checking applicant's postings on such sites
- be careful posting pictures of yourself if it could identify where you live, go to school or otherwise spend time. Being sociable online doesn't mean divulging every aspect of your personal life
- never post pictures that embarrass other people or show them partially clothed: this is especially true of images taken of other children. Sending your photo to chat rooms is also not a good idea and can be dangerous
- treat others as you would have them treat you: considerately and with respect
- be careful who you share information with and remember that a 'friend of a friend' may be no friend to you. Do not reply to messages from people you don't know and it's always best to keep your friends list to people you actually know as opposed to strangers
- report anything odd or disturbing – or instances of bullying – to an adult and the website itself
- if you are Twittering, be careful who you allow to follow you and make sure you don't post specific information about where you are going to be at any given time

Reporting abuse

If you see content on the Internet which you believe is illegal or in breach of a website's terms and conditions you can report it to the service provider, IWF and/or CEOP. To report abusive emails you need to contact the email service provider of the sender and more advice on how to do this can be found at orange.co.uk/help

Most websites offer ways to report abuse on the web pages, next to the content or profiles themselves. If you're not sure how to report abuse on a service you can try to get information using the site search engine and look out for links to report abuse, flag or report violation. In some cases the service will have sophisticated systems that capture the content automatically but in others you may need to send screen grabs or logs to the service provider. On receipt of a report the service provider should review the content and if there is a breach of the terms and conditions it could be taken down and in some cases further action could be taken against the poster.

What about illegal websites?

If you believe a website or images you have encountered to be illegal, you can report it the IWF:

You can do this on their website, via either:

- email to report@iwf.org.uk
- online at iwf.org.uk
- WAP (i.e. on a mobile handset) on wap.iwf.org.uk

The IWF website will also give you clear guidelines on what constitutes an illegal website or image.

If you believe that you have encountered suspicious behaviour towards a child you can report abuse directly to CEOP ceop.gov.uk

Aside from content that's clearly in breach of the law, it's important to remember that what's inappropriate to some may be acceptable to others which is why it's best to have Parental Control software on your computers at home so that you can set limits as to what types of sites can be visited.

gaming

It's also worth remembering that many games consoles such as the X-Box, Playstation or Nintendo Wii, have games that allow players to chat online in real time, get involved in role plays and build all sorts of social networks. The same risks apply here as with the Internet and its important that children understand that they should behave appropriately. Video games sold in the UK will in future all be classified according to the PEGI age-rating system & each will carry symbols to depict the type of content e.g. bad language or violence.

Social networking through online gaming is becoming increasingly popular and you may have heard the term 'Massively Multiplayer Online Role Playing Games' (MMORPGs). This is where a large number of users will interact with one another within a virtual world and games consoles can be used for chatrooms and instant messaging, whether engaged in game-play or not. There are some websites that allow you to build characters and take on a second identity and live in a virtual world and this can be an educational and entertaining activity for children.

Some games have the facility to report anything suspicious just remember to make sure that the games they are playing are age appropriate.

Remember: Other devices that connect to the Internet through wifi can also be used to access chatrooms, such as the i-pod Touch and of course a mobile phone. Check page 26 to see advice on how too stay safe in chat rooms.

phishing

What is it?

Phishing is the name given to scams where fraudsters attempt to trick a user into disclosing private information, such as credit card details, account names and passwords over the Internet. This information can then be used for illegal purposes such as unauthorised money transfers.

Note: Fraudsters can be very clever. They can design their site so that it looks very similar to a trusted service. They will even use a similar web address to make the site look all the more convincing.

How to avoid becoming a victim of Phishing

1) if you're asked to enter credit card or bank details in an email or online, be suspicious

- always use the url (dedicated link) supplied by your bank and be cautious following links in emails
- don't give your bank details by email
- if you are unsure about an email or pop-up call your bank to check

2) only enter your details on a secure site

All reputable Internet services including ours use the Industry standard Secure Socket Location (SSL) encryption when taking your credit card or bank details online.

Look for the padlock or unbroken key symbol at the bottom of Internet Explorer and the use of https:// rather than http:// in the web site address; this tells you that you are on a secure server.

3) top tips to help protect your computer

- install a firewall, up-to-date anti-spyware, anti-virus software and the latest security updates (patches) on your computer
- be alert when browsing the Internet. Certain websites for example, web sites hosting pornographic material or pirate software may include spyware which can steal your data

- if an advert tells you that your computer is not secure or you've won a competition, use the information as a prompt to update your existing anti-virus software and check that your firewall is turned on

The latest versions of Internet Explorer and Firefox (web browsers) automatically have anti-phishing software built in. Check your settings to be sure what version you have.

email scams

If you get an email telling you that someone needs your help to recover their fortune from a foreign bank or they need to use your bank to transfer funds this is likely to be what is known as a 'Nigerian scam' (or sometimes referred to as a 419). Fraudsters are very clever and make up stories to try to get you to give them your bank details so they can steal your money. If you are at all suspicious delete the email or report it to the senders email provider. The same goes for competition prize scams – the chances are if you didn't enter a competition in the first place you probably haven't won anything.

copyright and downloading

Copyright law applies to a wide range of creative and intellectual works online as it does offline. This means that you can't upload or download copyrighted material eg music, software, books or news articles without the copyright owners permission. Legal download services are available online for example Orange music store **jukebox.orange.co.uk**

how would I know if my child was illegally filesharing?

First and foremost talk to your child and explain the implications. Content such as music and film is commonly shared using peer to peer (P2P) networks such as Ares or Bit torrent. You can download free software that will help you identify music files and uninstall P2P software. Just go to **ifpi.org/dfc/downloads/dfc.html**

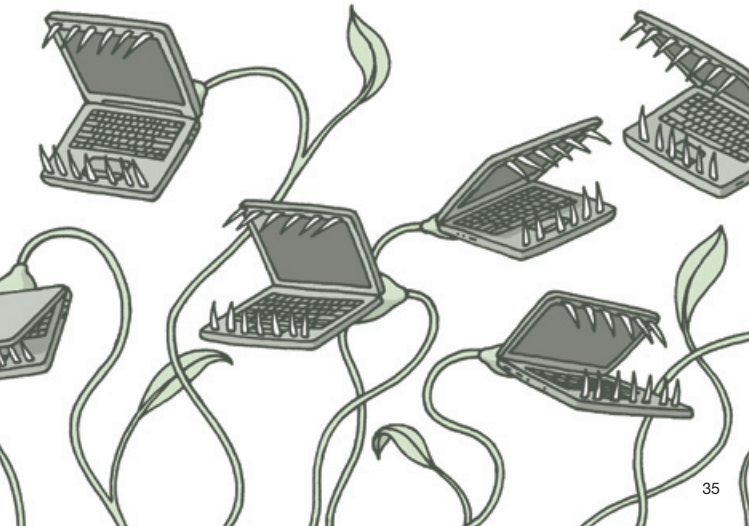
Remember:

- downloading and uploading copyright material is against the law
- many legal download services exist online
- there is no age below which copyright infringement becomes legal
- parents may be responsible for copyright infringement if their children use their parent's Internet connection for the purpose of copyright infringement
- there is a useful guide available at **childnet-int.org/downloads/CN_IFPI_MusicLeaflet.pdf**

plagiarism

Copying work and passing it off as one's own is known as plagiarism. Explain to your child that the Internet is a great source of information but that they should use it to help them create their own material. Schools and exam boards take a dim view of plagiarism and impose sanctions on students who are caught.

Sometimes plagiarism can be accidental as children are encouraged in some case to use the Internet to assist with homework. You can find out more about this at: **plagiarism.org**



quick reference guide – what you can do

Talk

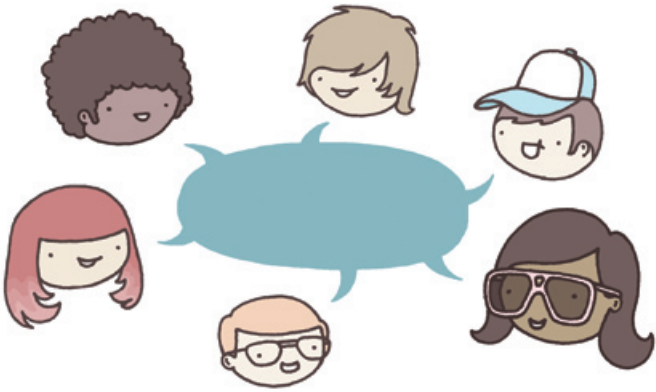
- chat to your children about what they do online and take an interest in their online lives
- discuss what the risks are and empower them to manage those risks themselves so they don't feel like they are being watched
- trust them to make sound decisions – our research shows they do know what dangers can face them, but often feel "it won't happen to me"

Act

- filter – as a basic step, make sure you have 'parental control' filters in place on your computer at home. Discuss privacy settings and help your child decide who they want to share information with
- check if your Internet Service Provider (ISP) can add parental controls to your service package. This will allow you to set controls about what type of sites your children can access and will restrict access to over 18 and adult content websites. Encourage your children to talk to you about their experiences online; many fear their access will be barred if they tell about something negative they have seen online
- talk to your school – e-safety advice is a part of the curriculum and they may also be able to offer you practical advice as well as keeping you informed about how your children are using technology in the classroom. Orange have a free educational resource for schools about staying safe online and text bullying. Teachers can order this through our website: orange.co.uk/education

Try

- have a go! Have you seen a social network site? Do you know how to ‘blog’? Perhaps you could try some of these activities for yourself and see what all the fuss is about. Set up your own social network profile and use it to get in touch with old friends or post some pictures and share them with family and friends. Most sites allow you to set privacy controls so that you only have to share things with people you choose
- why not do a web search for your favourite hobby or interest and see what discussion forums there are – you can contribute to debates, add information or even give advice to others and you might find that you can get in touch with like minded people



jargon

There are many expressions associated with mobile phones and the Internet and new ones appear with all the time. However, here are some of the expressions you may have come across:

WAP

Wireless Application Protocol. This allows users to receive information instantly via handheld wireless devices such as mobile phones, pagers, two-way radios and communicators.

3G

'Third generation'. This is a technical standard common across the mobile industry that allows very rapid data transfer. Such high data speeds enable a range of new services like video, Internet access and interactive services.

MMS

Multi media messages/photo messages – pictures and video you can send and receive with a mobile handset.

SMS

Text messages.

Bluetooth®

A form of direct device-to-device radio communications system. It is fitted to many mobile handsets and 'wirefree' headsets and allows phones to communicate when in close range of each other – without the use of the mobile phone networks.

Bluejacking

Some users with Bluetooth®-enabled mobiles use the technology to send anonymous text messages to strangers (nicknamed bluejacking).

Infrared

A type of invisible light that some handsets and other devices can use to communicate. Most TV remote controls use the same technology. It is an alternative to radio (see Bluetooth) but requires direct line of sight to work.

Ringtone

The old fashioned phone ring has been replaced on mobiles by a wide range of sounds from pop songs to actual recordings. Some are free, but most must be downloaded and paid for.

Screensaver

This is the often animated picture shown on phones that are switched on – but not in current use. Can be chosen and paid for.

Wallpaper

The usually still screen image behind a phone's various option lists can be downloaded and paid for.

Blog

Short for weblog where users can post information and write about anything and everything for others to see. Often updated in the form of diary entries, debates, news and pictures.

Wiki

A web page that allows anyone to contribute and edit pages with out the need for web design programmes.

jargon continued

And some things you might see or hear from your children…

OMG	Oh my god!
LOL	Laugh out loud
BRB	Be right back
ROTFL	Roll on the floor laughing
A/S/L	Age, Sex, Location
POS	Parent Over Shoulder
KPC	Keeping parents clueless
T+	Think positive
Rents	Parents
Newb	New user

Mods	Chatroom moderators (most sites are monitored for key words and do respond to requests for intervention where needed).
Troll	People who visit chatrooms with the sole purpose of annoying other chatters.
Flaming	Being nasty to other chatroom users in order to start an argument or debate.
WAP	Wireless Application Protocol – allows users of wireless devices to receive instant information.

useful numbers and contacts

Orange

Customer services (contract customers) 150 from your Orange phone or 07973 100 150

pay as you go customers 450 from your Orange phone or 07973 100 450

Orange switchboard 0870 376 8888

orange.co.uk for our main Orange website or orange.co.uk/safety for information about safety and security.

For child safety:

If you would like advice about a specific concern relating to a child, you can talk to one of these organisations who may be able to help:

NSPCC

nspcc.org.uk or call 0808 800 5000 if you are worried about a child.

NSPCC Registered Charity number: 216401

Samaritans

samaritans.org or call 08457 90 90 90

Samaritans Registered Charity number: 219432

Barnardo's

barnardos.org.uk or call 020 8550 8822

Barnardo's Registered Charity numbers: 216250 and SC037605

All three of these wonderful organisations are partnered with Orange and we actively support and fundraise for them. They all do great things to help protect children and if you know of a child that may be at risk they can help with advice and guidance on what you can do.

Other helpful organisations and websites:

CEOP

Child Exploitation Online Protection Centre –
To report online abuse or if you suspect a child may be in danger from someone they have met online.

ceop.gov.uk or call 0870 000 3344

CEOP run a great programme called 'Think U Know' that's for children, parents, carers and teachers and gives practical advice about the good and bad side of technology.

thinkuknow.co.uk

IWF

Internet Watch Foundation – The UK's hotline for reporting illegal content on the Internet.

iwf.org.uk

Childnet

This organistaion works to keep children safe on the Internet and they have their own resources giving practical advice to parents, teachers and carers. Check out their 'Know It All' programme on the website at:

childnet.com

This booket is printed entirely on recycled paper containing
100% post-consumer recovered fibre. You can recycle this publication again.

T1133 OPM131823 07/09