Staying Safe Online: Get the facts

Advice for young people about dangers and risks online

The internet is certainly a valuable and fun resource for instant entertainment, sharing media, meeting new people, keeping in touch and a phenomenal learning tool; however, with this technology comes great responsibility.

The internet poses a significant amount of risk from various forms of illegal activity, ranging from bullying, indecent images, through to fraud; people on the internet aren't always who they seem.

In the same way you learn about safety when you leave the house, it is important to learn how to stay safe online and to use these are skills throughout your life.

Golden Rules

* Don't send pictures of yourself to anyone, especially those of a sexualised nature
* Don't become online 'friends' with people you don't know
* Don't give out personal information such as your address or phone number
* Don't open emails or attachments from people you don't know
* If anything you see or read online worries you, report it or tell someone
* Never arrange to meet someone in person who you've met online

Social Networking

Social networking sites and apps, such as Facebook, Twitter, Instagram, Tumblr, and SnapChat, have become incredibly popular in recent years. Most users are genuine, but because it is so easy to hide behind your real identity, it is highly possible to behave in a way you wouldn't normally and chat with people you would probably choose to avoid if you met in person.

Privacy

The internet offers users a lot of freedom; this can lead some people to share information and behave in ways they would not in public/real-life, such as:

* Say things on a status update / post / tweet they would never say face to face
* Give out personal information about themselves or others that they would normally keep private (including photos)

An example of how this may go wrong: a person wants to let their friends know about a last minute party they are hosting by posting the information about it on social media; this leads to lots of other people finding out about it and turn up uninvited. The party gets out of hand, people get angry and the 'gate-crashers' refused to leave; the police attend and close the party down.

Cyber bullying

Cyber bullying has the same effect as face to face bullying; the victim can be made to feel frightened and alone, while the bully attacks from behind a screen and hides to avoid being identified or held to account. Often cyber bullies feel braver because they can't be seen, but it can actually be the most traceable form of bullying because there's actual evidence that it happened.

Posting comments, images and videos about a person online causes a victim to feel frightened and upset
Cyber-bullying can encourage others to become involved; in some cases the attack can become viral
Cyber bullies can hack a victim's personal accounts and harass them from within their own user profile
Anonymous threats can leave a victim feeling scared for their safety

Cyber stalking (harassment online)

Harassment on the internet can be just as frightening as being physically stalked in real-life. Females are more commonly victims of this behaviour, but males are also at risk; a common scenario being an ex-boyfriend or girlfriend who is upset about the end of the relationship.

Cyber stalking may take place when an online friendship/relationship turns sour; the perpetrator may constantly message you or others close to you causing distress and/or anxiety. They may also stalk you by watching your online activity without you being aware; this can also happen entirely at random, by an online stranger

Identity Theft & Fraud

The more information you place online, the more at risk you become of identity theft; this can often happen by opening or replying to an email or attachment from an unknown source, and by posting personal information on social networking sites.

Personal information you should **not** make available online or give out through unsafe sources:

- card/banking information
- email address
- passwords
- phone number
- photos of yourself
- postal address

The consequences of fraud can be serious; therefore you should be aware of the risks, if someone steals you or your parent's identity they can commit serious offences such as:

- commit crimes that you or your parents could get into trouble for
- create a profile using your details to commit offences against others
- steal your/their money
- take out loans/credit in your/their name

If you are not sure – ask your parent!!

Sexting

Sexting usually refers to sending and receiving messages, photos or videos of an indecent or sexual nature; these include:

- Images or videos of a sexual nature
- Naked pictures
- Sexually worded texts
- 'underwear shots'

A common scenario is when images or videos are shared between boyfriend/girlfriend or friends; also sharing them with someone they have met online with no idea who they are really sharing them with.

Reasons people 'sext':

- Being harassed, threatened or blackmailed to do it – it's easier to give in
- Feel pressured to 'prove' you're willing
- Feel they 'owe' it to their boyfriend/girlfriend
- It's ok because they're in love with the person and trust them
- Made to feel guilty if you don't do what they ask
- Their friends are doing it
- They feel proud of their body and want to show it off to other people
- Wanting to fit in with in with friends

Remember!!

There is no turning back once you press send

If you use apps like Snapchat, people can take screen shots to capture the image

You risk giving the wrong message and be judged as someone you are not

You may attract unwanted attention, resulting in cyber-bullying or cyber stalking.

Inappropriate content

Be careful when visiting certain sites, many of them feature sex, violence, abuse and other illegal activities; access is still possible with filter/parent controls in place. You may also be forced to view inappropriate content through what is posted on other people's social networking sites.

Online grooming

Online grooming is a term to describe inappropriate behaviour towards a young person, putting them at risk to a sexual offence. As already stated, the internet allows people to communicate with each other through chat forums, social networking sites, mobile apps and interactive games.

Sex offenders commonly use these sites to contact young people by posing as young person; this disguise helps them communicate with young people to gain trust with from them and their friends. This 'friendship' is based on lies and deceit and is often mean to encourage sharing of images/information and in some cases arranging to meet in person.

Making 'friends'

It seems that the more friends you have online the more popular you are perceived to be; this creates a pressure for young people to 'add' people to their contacts too easily and without knowing them in 'real-life'. This can be risky!

Although some people like to boast about how many 'friends' they have on their social networking site, remember that real friendships aren't made by computers.

Remember!!

Friendships made online are made by clicking a button rather than talking to people and sharing experiences

Being online 'friends' with someone can be less meaningful than face to face friendship

You can easily fall out with an online 'friend' because of misinterpreted comments

It is far easier, and healthier, to sort out disagreements and problems when you can talk to someone face to face

E-mails, Spam &, Phishing and Viruses

Spam: unsolicited bulk messages, especially advertising.
Phishing: the act of attempting to acquire sensitive information such as usernames, passwords, and credit card details.
Viruses/Adware/Malware: programs that may be harmful to your computer.

Beware!!

An email from someone you don't know who could be trying to sell you something, transmit a virus or send abusive or explicit content

If it is spam, you might become a victim of fraud

If it is a virus, your computer might get damaged

If it is abusive or explicit, it might upset you or even get you into trouble

If it has an attachment, beware that it might contain a virus or something you don't want to see; this may mean you will have to pay to have it removed from your computer

You can avoid unwanted emails by getting the right software; ask an adult to help get this set up.

The golden rule is, if the email is from someone you don't know, delete it!!

Tips to keep you safe

Below are some points we advise you follow to keep yourself safe when you are online and when using social media.

Make sure you're old enough to sign up and use a site

Consider using a made up name or nickname on your profile

Never give out personal information

Don't add friends you don't already know personally

Use an email address that does not include your name

Always use a 'strong' password; don't use any names or words that someone might guess, like the name of your dog or your favourite singer. Use random letters or numbers and change your password regularly.

Pictures and videos can be shared very easily across the internet; make sure you are very careful when uploading. Even if you only share it with friends, it can easily be passed on to others

Be very careful about sharing content online, especially if it isn't yours to share. Illegal downloads are definitely best avoided.

Never meet up with anyone you have met online

Make sure you know about the safety features on networking sites; some have a 'panic or report button' which you can use if you see something that shouldn't be there

If anything happens online that you don't like, tell someone

Help & Support

Below are organisations that can give you information, help, advice and support

Get Safe Online

www.getsafeonline.org

Free expert advice on how to protect yourself, your computers and mobile devices and the basics of safe surfing and avoiding internet crime

CEOP THINK U KNOW .co.uk

www.thinkuknow.co.uk

A web site offering age appropriate games, videos and information about the internet; find out what's good, what's not and what you can do to stay safe; report online incidents that make you feel worried or uncomfortable

fearless be fearless against crime

www.fearless.org

If you know someone who is carrying out any form of cyber-crime, you can report them anonymously through Fearless or CrimeStoppers

CRIMESTOPPERS 0800 555 111