



KEEPING YOURSELF SAFE ONLINE



How to Keep Yourself Safe Online

- ☞ Be aware of safety information and tools on the site you are using and use them.
- ☞ Don't share too much personal information.
- ☞ Be open with parents/carers about using the internet and about why you shouldn't speak to certain people.
- ☞ Be specific about what you are searching for on search engines.
- ☞ Don't accept friends unless you know them in the offline world—make use of being able to see their profile temporarily to check it is who you think it is.
- ☞ Don't argue with people online, sort things out face-to-face.
- ☞ Remember that the Internet never forgets what you post on-line.
- ☞ Change your password regularly.
- ☞ Log out when you have finished.
- ☞ Don't share inappropriate photos or ones which show where you live/ work or go to school.
- ☞ Don't post where you are on status.
- ☞ Know where to get Internet Advice.
- ☞ Don't tag yourself in pictures.

PROTECT YOUR OWN SAFETY

The 'Click Clever Click Safe' code is a list of three simple things to remember when you're online:

- ◆ Zip it
- ◆ Block it
- ◆ Flag it

Zip it



When you're online, always keep your personal stuff private and think about what you say and do.

Remember that people online may not be who they say they are. Online friends are still strangers even if you have been talking to them for a long time.

Don't share personal information online. This includes:

your full name

photos

addresses

school information

telephone numbers

places you like to spend time

Make sure you have set your privacy settings to restrict access to personal information.

When you use chat rooms or instant messenger, use a nickname instead of your real name.

To stop people accessing your online accounts, always keep your passwords secret and change them regularly.

Block it



Think about blocking people who send you nasty messages and don't open unknown links and attachments.

Always delete emails from people you don't know, and don't open attachments from people you don't know. They might be nasty or contain a virus that can stop your computer working.

If someone is mean or sends nasty messages online, block them.

Flag it



If you see anything that upsets you online or if someone asks to meet you, flag it up with someone you trust.

If you are worried or unhappy about anything you see online, tell a parent or an adult you trust and they can help you.

If a friend you have made online asks to meet you in the offline world, talk to your parents or a trusted adult about it. You should never meet up with someone you have met online without an adult going with you because it is dangerous.

If someone you know is being nasty to someone online, speak to a parent or trusted adult about it.

USING THE INTERNET

There are lots of sites around that allow you to talk to other people on the Web. Chat rooms give you the chance to have a conversation with other people and get instant replies. Online message boards and forums let you post questions or comments and ask other users to give their opinion in their own time. There are also social networking sites like Bebo, MySpace and Facebook.

It can be a great way to chat to other people who share your interests, but you should always be careful not to pass on any of your personal details. You should always keep in mind that internet users can pretend to be anyone they like. They can lie about their age, their interests and whether they're male or female. No matter how long you've been chatting, remember that they're still strangers; you don't really know them at all.

What information to give out

Be careful what information you give out on your profile. Remember that you don't know who your friend's friends are ... or your friend's friends' friends! And you don't know what they'll do with your picture or your phone number if you give it out by mistake. Once your picture is out there, it's out there forever and you won't be able to get it back.

Be aware that information on your profile could potentially be viewed by anyone. So if you wouldn't be comfortable printing it off and handing it out on the street, maybe it shouldn't be on your profile.

Use a nickname or your initials instead of your name – you don't want just anyone knowing who you are. Consider changing your photo to a cool graphic that way strangers won't have access to a picture of you. It's not a great idea to post where you're going on your profile or twitter or where you live. Think through if you'd want everyone who can view the post to turn up at any time!

Who to Chat to?

Think through who you want to chat to and how many of your personal thoughts you want anyone to view. Sometimes, it can seem a good idea to share what you got up to with your boyfriend last night, or the argument you had with your best mate; but as you're writing – remember that information could be public forever! It is tempting to share loads of stuff on your profile, especially since you're often typing from the comfort of your own home. But remember, the Internet is a public space. Test yourself by asking "would I want my teacher/Mum/Dad/ stranger on the train to see this?!" If the answer's no... don't post it!

Who to Accept

Be careful who you agree to accept into your forums / private chat areas. Unfortunately because there are so many young people using these sites, adults with bad intentions will use them to make contact with children too; so you're safer to only chat to people you know in the real world.

If you know someone... who knows someone... who knows someone, it doesn't make them your friend, so think carefully about whether you should be chatting to them and what kind of things you're saying.

Privacy Settings

Use your Privacy Settings. Adjust your account settings (sometimes called "Privacy Settings") so only approved friends can instant message you. This won't ruin your social life – new people can still send you friend requests and message you, they just won't be able to pester you via IM. This means that people you don't want to see your profile can't!

Some social networking sites are really well run and the administrators will try to help you remember to keep your personal information to yourself. Others are not so good – so be careful when choosing which areas you go to.

Pictures

Only upload pictures that you'd be happy for your mum to see – anything too sexy to be passed round the dinner table should NOT make it onto the web, as you don't know who could be looking at it or what they might be doing with it.

Don't post your phone number or email address on your homepage. Think about it – why would anyone actually need this info when they can message you privately via your social networking site?

Don't post pictures of you or your mates wearing school uniform – if dodgy people see your school badge, they can work out where you are and find you. The more anonymous you are, the less vulnerable you are to people with bad intentions.

Tick the "no pic forwarding" option on your settings page – this will stop people forwarding your pictures to anyone without your consent

Blogging

Don't give too much away in a blog.

Yes, tell the world you're going to a party on Saturday night. But don't post details of where it is. Real friends can phone you to get details, why would a complete stranger need to know this information?

Video

Remember that any video uploaded on the net could potentially be there forever for anyone to see; that includes your parents, teachers, future university or employer! Also remember that if you post films with you or your friends in them, you are allowing people to potentially find out information that you wouldn't normally share.

Think about whether your clip identifies you, your school, and the place you live or puts your friends at risk before you post it.

Video hosting sites like YouTube do have the ability to take down inappropriate or offensive content. The video will need to be illegal or to have broken the terms and conditions of the site. On YouTube you can report by creating an account and logging in, once you have done this—you can 'flag content as inappropriate'. This option can be found under the video itself.

Sexting

Someone taking an indecent image of themselves, and sending it to their friends or boy/girlfriend via a mobile phone or some other form of technology is sometimes referred to as 'sexting'.

Once these images have been taken and sent to others, control is lost of them and they can end up anywhere. They could be seen by friends and family, a future employer, or even, in some cases, end up in the possession an offender!

This also puts that person who originally sent the images in a vulnerable position, as somebody they may or may not know now has these images and could use technology to bully, harass or even try to locate them.

Just think – if you wouldn't print and pass these images around your school or show your mum or dad, they are not appropriate to share via phone or other technologies.

MOBILE TELEPHONES

Your Number

It is a good idea to only give your number out to friends who you know in the real world. If your mobile number is given to people that you don't know they may try to hassle you. Never put your mobile number on your social networking site.

Camera Mobiles

Having a camera on your mobile is fun very useful but be careful if you share your photos with others. Pictures can be changed and shared around, so think about what the image is and who you are sending it to. Once out in cyberspace it is there forever!

Bluetoothing

This is a quick and easy way of sharing stuff like photos, music and other files. It is important to lock your Bluetooth otherwise anyone in the area can access things in your phone, like your contacts.

GPS Tracking

It is worrying to know that social networking using GPS technology means that your contacts will be on a map, showing exactly where they are. This means they also know exactly where you are: scary if you do not know or trust them. If you want to use these sorts of apps you need to use your privacy settings and remove anyone that you do not know or do not trust from your contacts.

Harassment

If you are receiving unwanted or insulting texts, you can contact your service provider. If you think you are being targeted by other people and they are upsetting you, this is cyber bullying and you should also tell a trusted adult, like your parents or a Head of Year.

WHO CAN HELP IF YOU ARE WORRIED

Talk to an adult that you trust

If you feel comfortable talk to an adult you trust such as a teacher, your Head of Year, or a relative.

Talk to someone in confidence

You can always talk to Childline, a confidential helpline run by the NSPCC. You can call them on 0800 1111 or go online at www.childline.org.uk.

Report it

If you are worried about something that is happening to you online you can report it through CEOP (Child Exploitation and Online Protection Centre) - there is a button you can click on our College Website. CEOP is staffed by specialist police officers, social workers, counsellors and investigators and your report will go straight to them.

Other people who can help you

Content that you have seen online and which you think may be illegal should be reported to the Internet Watch Foundation (www.iwf.org.uk) who will contact the police if necessary.

If you are being bullied online you can find more information and advice on cyber bullying at www.beatbullying.org.

The site www.thinkuknow.co.uk is a very good site and has a great deal of information and help for any online worries you may have.

Other useful websites for you and your family are:

www.getnetwise.org

www.getsafeonline.org

www.kidsmart.org.uk

www.digizen.org

www.safesocial.com