Cybersafety and protocols for conducting online life?

Sunderland is an exciting place to live.

We lead the way in making use of services online. We are one of the most connected cities in the UK.

Whatever devices we use - going online allows us to access information whenever we need and stay in touch. One of the biggest challenges you face is guiding them to towards using their gadgets safely and responsibly.

The 'Cyber Safe' agreement has been developed to help you to support your child.
It includes issues they could face and how to avoid them. It is suggested that your whole family will provide a positive example to follow. You could do this by demonstrating how you stay safe by following the agreement too.
It is something that we hope you will all follow when using online services and mobile technology wherever you are to ensure that everyone enjoys the time they spend online. The aim is for Sunderland to be one of the most connected cities and also the safest place to be online in the UK.

The Cyber Safe Agreement

The agreement is based on advice given by organisations that help young people stay safe online. We have taken the best of that advice and turned into a set of statements for our young people to follow.

1. Accept good communication

Part of being a good communicator is not to accept bad communication from others. No one likes to receive a message that upsets them. If you receive a message that upsets you, the first thing you should do is to check you have understood what the sender meant. Think what else this might mean. It is easy to misunderstand and be hurt by a message when the person who sent it didn't really mean for that to happen. The person may have been in a hurry when they were sending it.
If you aren't sure what the sender meant, ask them in person. It's much harder to misunderstand someone's communication if you talk on the phone or meet them face to face because you can tell by the expression in their voice or their use of body language.

If you do receive a message that really upsets you – and it is obvious that the person meant for that to happen then you should keep it and contact someone who is able to help. It may be one of many messages they send. This type of message is described as "Cyber Bullying." The best way to avoid this is only to share contact details with people you trust. Keep your Email address or mobile number private, then they won't be able to contact you.

Websites like www.cybermentors.org offer advice. If the bullying is happening by phone, contact the mobile phone company. All UK mobile operators have nuisance call centres and procedures in place to deal with such incidents.

They may help you to change your number or, with help from the police, take action against the bully.

Here are the contact details for mobile operators:

O² - Call 08705214000 or email ncb@O2.com or visit this part of the website http://www.o2.co.uk/support/generalhelp/howdoi/safetycontrolandaccess/nuisancephonecalls

http://sunset.o2.co.uk/services/childprotection/nuisancephonecalls

Vodafone - Pay Monthly customers call 191 from a Vodafone phone or 08700700191 from a landline

Pay As You Go customers call 08700776655

Or visit this part of the website http://help.vodafone.co.uk/system/selfservice.controller?CMD=BROWSE_TOPIC&PARTITION_ID=1&CONFIGURATION=1000&SIDE_LINK_SUB_TOPIC_ID=1069&SIDE_LINK_TOPIC_ID=1007&TOPIC_ID=1069&TOPIC_TYPE=0&STARTING_ID=0&TOPIC_NAME=Dealing%20with%20nuisance%20calls&PARENT_TOPIC_ID=1007&SOURCE_FORM=BROWSE_TOPIC

Orange - Pay As You Go customers call 450 on Orange phone 07973 100450 from a landline
Pay Monthly customers call 150 from Orange phone or 07973 100150 from a landline

http://www1.orange.co.uk/safety/mobile/156/160.html

Three - call 333 from a 3 phone or 08707 330 333 from a landline

TMobile - call 150 from TMobile phone or 0845 4125000 from landline or visit www.tmobile.co.uk and use the 'how to contact' section of the website

http://www.t-mobile.co.uk/help-and-advice/advice-for-parents/bullying/

If the bullying is happening by Email contact the provider of the Email address that the bully is using.

For example if the bully uses an @hotmail.com address contact Hotmail.

By only accepting people you know as friends on social networking sites such as Facebook and MSN, this helps to lessen the chance that these services can be used to bully you too.

If someone chooses to Cyber Bully you, they may be breaking a few different laws meant to protect your privacy online so it is worth contacting the services above or the police to put a stop to it.

These are four UK statute laws and one Scottish common law that are link to the use of IT in relation to bullying:

The Protection from Harassment Act 1997

The Act states that it is unlawful to cause harassment, alarm or distress by a course of conduct and states that 'A person must not pursue a course of conduct, which:

- amounts to harassment of another
- he knows, or ought to know, amounts to harassment of the other.'

The Criminal Justice and Public Order Act 1994

This Act defines a criminal offence of intentional harassment, which covers all forms, including sexual harassment. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, he/she

- uses threatening, abusive or insulting words or behaviour or disorderly behaviour; or
- displays any writing, sign or other visible representation which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

The Malicious Communications Act 1998

Under this Act it is an offence to send an indecent, offensive or threatening letter, electronic communication or other article to another person. Under section 43 of the Telecommunications Act 1984 it is a similar offence to send a telephone message which is indecent, offensive or threatening.

Bother offences are punishable with up to six months imprisonment and/or a fine. The Malicious Communications offences are wider ranging, but under the Telecommunications offences, it is likely that the Police will use the former Act to bring a charge.

The Communications Act 2003

The Communications Act 2003 is by far the most recent Act to be passed. Section 127 states that a person is guilty of an offence if s/he

- sends by means of a public electronic communications network a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or
- causes any such message or matter to be so
- A person is guilty of an offence if, for the purpose of causing annoyance, inconvenience or needless anxiety to another, he
- by means of a public electronic communications network, a message that he knows to be false,
- causes such a message to be sent; or
- persistently makes use of a public electronic communications network

Breach of the Peace (common law)

Breach of the Peace is Scottish common law. At present behaviour in Scotland which might be described as harassment or stalking is usually prosecuted as a breach of the peace. This common law offence covers all behaviour (including single incidents) which causes, or is likely to cause:

- Fear, alarm, upset or annoyance
- When one or more persons conduct themselves in a riotous, or disorderly manner, anywhere, which alarms, annoys or disturbs other people
- The offence can take place anywhere (a house, an office, a school or a public street)
- The element of disturbance would be the most relevant to Cyberbullying as the behaviour does not have to be noisy but still of a nature that would cause concern to other people – harassment or stalking and bullying

The Courts recognise that breach of the peace can be serious and a life sentence is theoretically possible. A sentence of eight years was recently imposed for the crime of Breach of the Peace.

It is worth noting that the age of criminal responsibility in Scotland is eight. All organisations, including schools are covered by the laws stated above. If an offence takes place in school it is still an offence.

Top Tips:

If you can, block the bully, and don't respond. Remember to keep a copy of any messages. They will soon get bored if they don't get a reaction.

Never forward anything that someone sends you if you think it will upset someone. You don't want to become a Cyber Bully yourself.

Helplines:

a) Childline free 24hr. helpline for children & young people 0800 1111
b) Kidscape – advice exclusively for parents & carers on bullying 08451 205204
c) Get Connected – free confidential helpline for young people 0808 8084994
d) Samaritans – 08457 90 90 90

Useful Websites:

a) Childnet - a range of resources for families & schools www.childnetint.org
b) Cybermentors - Talk to a someone who is trained to help you at www.cybermentors.org.uk

2. Be a good communicator

When we are talking face to face it's easy to see from a person's expression whether they are joking or being serious. When we are communicating electronically (using text, Email and Instant Messages), it is very easy for people to get the wrong impression. Sometimes these messages can cause a lot of upset that was not intended.

This is particularly important when we post things on sites like Facebook. Remember that status updates, messages and comments can often be seen by many more people than the person we send it to.

Ask yourself "Would I write this on a piece of paper and put it on a notice board in the Bridges?" if the answer is no rethink your message or send it in a different way.

We all know that bad news travels fast. If you have been the victim of gossip or rumour, it can be really upsetting. Using services like Facebook, MSN or Blackberry messenger to pass on information about others can mean that the upset caused can have a much greater impact as it can be spread

quickly. It is amazing how fast you can become a cyber bully without even meaning to, simply by passing on some private information about someone else.

Encourage your child to put themselves in the position of the person they are sending a message to. Read through it and ask yourself "What other meaning could they give to my message?"
"Is the intention of my message clear?" A message should never be sent if it there is the possibility that it could be interpreted that your intention is to upset or hurt someone.
This isn't always easy when we are sending a quick message when we are in a rush but it's worth taking the time to make sure that we are good communicators.

It is important to only share your contact details with people you trust and never to post your email address or phone number in a public place. Thinking back to our earlier example of the noticeboard in The Bridges. If you wouldn't put it there don't put it online.

3. I will be careful who I accept as an online friend.

Social networking is an important part of our use of the internet and making friends online is something that a lot of young people enjoy doing. While they are aware of stranger danger in real life they don't often apply the same principles to people they connect with online. They may not think of an online friend as a stranger and share private information with them without thinking of the consequences.

In order to minimise the risks of being targeted by online predators, there are some simple rules to follow:

- Choose usernames that will not invite inappropriate attention. Never use your full name or the name of your friends. Usernames like sexygirl14@hotmail.com suggest certain things about you to others that may cause you problems.
- Make sure your online friends are people who you know in real life.
- Keep personal information private.
- Change your settings privacy settings to "friends only" so that only your real friends can view personal information.
- Be careful who you add as a friend and remove anyone you don't really know.

Often there is competition between children to have the most 'friends' on social networking sites such as Facebook. This can lead to people not knowing everyone on their friend list.

Remember that TVs and IPods and games consoles can also be used to connect with other people while playing games. Check any device your children could use to connect to the Internet has the privacy settings set to friends only. Many devices have text and voice chat as well.
Always know who you are talking to. You can't always tell the age of the person who you are communicating with and young people can be tricked into meeting people they have only chatted to online. Most devices have parental controls so you can limit your child's access to certain features that may put them at risk. Switching off the text and voice chat is one of the options that you could use to restrict your child's access to inappropriate language.

Top Tips:

On line communities are a great way for young people to interact with others, however these communities may contain Cyber bullies, criminals and those people wishing to exploit young people.

Try to keep any device that can connect to the internet in family areas like the living room. This allows you to monitor what your children are doing online and look out for inappropriate behaviour from others. Regularly talk to your child about what they are doing online.

4. Be careful what you post

If we want to, we can share every aspect of our lives online. Sites like Facebook, Twitter and YouTube allow us to share where we are, what we're thinking, and pictures and videos of what we are up to.

If family and friends are in different areas of the country, it is a great way of keeping in touch and sharing your lives with each other.

To avoid problems, we do have to think carefully before we post photos and videos online.

For example: Everyone may have been really amused by that video of your cousin doing Wii Fit hula hoop but would your cousin want everyone on the planet to be able to watch him doing it on YouTube in ten years' time?

How many photographs and videos do you have in your family collection that you wouldn't want the world to see? That one of you trying on your mother's high heels when you were four?
Very amusing at the time but deeply embarrassing once you are an adult.

Some of the most popular videos on YouTube have been of children doing amusing things. One of the most popular of all being the one showing baby Charlie biting his big brother's finger.
It consistently features in the YouTube top ten along with professionally made pop videos possibly because of Charlie's evil chuckle when he realises his big brother is in pain.

Consider this:

Was it really a good idea for the parents to post it?
Is it good for Charlie and his brother to ***always*** be there for people to see even when they are grown up and looking for jobs in the future?

If you are posting videos and photos of people ask yourself whether you would ***ever*** regret people seeing it? If there is any chance that that you may regret it - then don't post it up there. If you really do want to share pictures with your friends and family find and use the privacy settings on the site to make sure that only they can see and download them. The same is true of photos and videos we take of other people.

Think about why you are putting it online and if you are posting something to make fun of someone then really you shouldn't be posting it at all or you may become a Cyber Bully without ever meaning to. If you aren't sure if they will see the funny side ask them.

It is easy to forget that anyone can see, download and change any image or video that we post online. By the time you change your mind and delete something from a site many thousands of people could have downloaded it and any one of them could do what they like with it and post it back without your permission.

We have to be very careful what we say online too. The Internet is a very public and open place, so putting something online that criticises someone or shares private information about them could be breaking the law especially if the comments are about their race, gender or sexual orientation.

It is never a good idea to make videos or images that would show more of you or your children than you would usually be comfortable with exposing at the beach or swimming pool.
The law on this is a bit of a minefield and it is very easy to find yourself doing something illegal without even realising it.

For example if a child took this kind of image of themselves, and sent it to a friend the same age, they could both be guilty of serious offences. If they are over ten years old they could also be prosecuted. If you or anyone you know receives an image like this the best plan is to delete it and warn the sender not to send any more.

It's not just video and images that we have to be wary of - the same goes for video chat using a webcam. It is astonishingly easy for someone to record on their computer what you send to them from your webcam. If they do, you have no control over what happens to the recordings or where they end up. They can even be sent to someone else over their webcam software so they think they are talking to you. Keep your webcam conversations clean and only cam with people you really trust like close friends and family.

It's worth taking a few minutes to look at the camera settings so you know how to turn off the webcam.

5. Be careful what you share

Many young people create and use social networks on line. Friends groups are created. Sharing information such as photographs can be done very easily. If a person's profile is set to open, then all groups of friends have access to everything and the content is not always appropriate.

Young people are often not aware that they post online can be viewed by anyone with access to the internet. They cannot delete something once it has been uploaded. A rule to follow is to only share as much detail as you would share with someone face to face such as your Grandmother or boss.

Phishing is where people are contacted by cyber criminals, encouraging them to link to a fake website and enter private information like their bank and credit card details. This can lead to your identity being stolen and criminals running up huge bills on your accounts.

Banks will never to ask you to give out personal details by telephone or email if you are in any doubt don't give it out.

Young people should be smart about posting photographs which, if they aren't careful, can reveal a lot of information about themselves. Look at things such as school name badges on uniform, street signs, car registration plates. Individually these pieces of information do not give much information about someone. When these pieces of information are put together, like parts of a jigsaw, they can reveal a lot of information like the school they attend, the area they live or where they will be at a particular time.

The same applies to information you put into your profile, things like your favourite bands and how you like to spend your time, can be used by online predators to help them to pretend they have things in common with you. They may use this to earn your trust and eventually persuade you to meet up with them.

We should always consider what we post if we are adding any information to social networking sites like Facebook. If your profile is set to public and an event is posted where you arrange to meet up with friends at a specific time and place, anyone visiting your page would also be able to turn up and join the party. They may not have the same intentions as the group of real friends.

Sharing information also covers passwords. Passwords are personal and should be kept private.

Follow these simple tips:

- Think carefully before you share any information, consider would I put the information on a huge sign outside my house for everyone to see?
- Treat your password like your toothbrush, don't share it with anyone and change it regularly.
- Remember the Internet never forgets and anything that you post online, could come back to haunt you in the future.

6. Be careful who you meet.

Encourage young people to understand that a friend is someone who you know because you have met them in person and got to know and trust them. An online friend is simply someone we agree to connect with online.

Online friends should really be treated as someone we've just bumped into in the street when we are choosing what we share with them. We should never agree to meet with our online friends unless we take our trusted adult with us.

7. Listen to your feelings

Often we use the internet in places where you feel at ease and relaxed. When we feel safe and secure we often share more information about ourselves than they would if we met someone in the street.

If we hear footsteps behind us in a subway late at night we may feel uneasy. While we are less likely to experience that feeling when we are chatting to someone online we should always trust our instincts if the conversation starts to makes us feel uncomfortable we should save it, end it and report it.

Encourage your child to tell a trusted adult if they ever feel awkward, embarrassed or worried by anything that they are asked to do or say by an online friend. Then the trusted adult can help them to take the appropriate form of action depending on the seriousness of the concern.

Many websites include a report abuse button. If you can't find one you can access it here www.thinkyouknow.co.uk

8. Make sensible choices

It is often said that the internet is a place where you can find proof that anything is true. Most of the content is open, meaning that anyone can access the information at any time. It can happen that young people access websites or play games that are not age appropriate.

Help your child to understand that not every website is meant for them and that not all information they may see on the web is true. If you show them some hoax websites this may help.

It is really important to help them understand that there are reasons why games have age ratings. Often children will say all their friends have it as a reason why they should be allowed to have it. Remember that there are specific reasons why the age ratings have been given to certain games. If you aren't sure, it's a good idea to play the game yourself and make your own choice about whether you want your child to play it. Remember that younger brothers and sisters will want to play it and may be able to see it too.

At school there are filters in place for making sure that students have no access inappropriate websites. When your child is using the web elsewhere they need to understand that it is never appropriate to access certain types of sites. They should also never try to get past the filters at school. It is a good guide that if it is blocked at school they shouldn't use it at home.

We want everyone to make informed choices when accessing different websites on the internet, thinking about who the site was made for and why can help us to decide whether it is a good source of information. It is important for the young people to be responsible about the sites that they visit, if they aren't sure that a website is suitable, the message is to not access it at all.

http://www.commonsensemedia.org/ gives excellent advice on this and if you find a site that you think is inappropriate you can report it to the Internet Watch Foundation at http://www.iwf.org.uk/