Be safe and keep others safe when online!

By Louise Jones

Background to the Highland E-Safety Group

The Highland E-Safety Group has been established since 2008 and since then has provided a range of advice, guidance, publications and training for anyone living, learning and working in Highland. The award-winning group is a partnership between Highland Council's education, culture and sport service, Northern Constabulary, Fujitsu, NHS Highland and High Life Highland.

Changing world of technology

Did you know that the internet recently celebrated its 21st birthday? Yes - the internet has come of age! That means we now have our very first generation of adults who have genuinely grown up with the internet since birth and wow, what opportunities this has brought us for living, learning and working. Almost every aspect of modern life has some kind of connectivity to a digital world and if it doesn't there will be soon be an "app for that"! With this in mind it's important that we all know how to make the most of the benefits of modern technology and also have to use it safely and responsibly.

Whilst we know it's vital to acknowledge the benefits we also know that being able to use the tools and ways of communicating now available freely to us, we need to have good programmes of education in schools. Highland schools now focus on educating pupils to be safe and also use online tools for their learning. The Highland E-safety Group also supports schools in working with parents and carers to support them in keeping their children safer online.

Since 2008 the E-Safety Group has had to be agile and responsive to the changing world of technology focussing on not only the dangers with strangers element, but also abuse online and personal information that we might put on about ourselves that may come back to bite us. We could only dream of what technology had to offer five or 10 years ago, so what might the future hold? We need to start preparing our children now for technologies that don't yet exist. This is possible by teaching them early on in life skills for living in a modern digital world and essentially instilling good habits for being safe, healthy and well and to be able to contribute to safer online experiences by being a responsible digital citizen.

Cyberbullying *is* bullying

There have been lots of articles in the press recently about cyberbullying and online abuse. During the Olympic Games articles in the news about some of the athletes being victims of cyberbullying showed us that anyone can be targeted online by hurtful and abusive behaviour, no matter who they are or what profession they are in.

Being targeted by cyberbullying, which is the use of mobile phones or technology deliberately to upset someone can be very distressing. The audience can be very large and reached rapidly. The difficulty in controlling electronically circulated messages means the scale and the scope of cyberbullying can be greater than other forms of bullying behaviours. Most adults can recall hearing or seeing hurtful comments about themselves or others during their own school days; imagine is those comments were available for the entire world to see and also impossible to erase or paint over.

Cyberbullying may also involve recording/videoing events without permission and uploading them to the internet, videoing events on mobile phones. This may also be a good discussion point with your child. By using their mobile responsibly this also helps to contribute towards being a good role model for siblings or others in online communities.

If your child receives abusive calls or messages, it is important that they do not respond. They should be able to tell this to you as their parent or carer or maybe another family member. It is advisable they do not delete or tamper with the message or evidence so that vital evidence is kept in case it does become a police matter.

As we have seen with some of the high profile cases, the police do take this sort of abuse seriously and with more modern traceable routes, it is difficult for the person being abusive to hide behind anonymity the internet may have afforded in the past.

Mobile phones and mobile devices

The Highland E-Safety Group also provides advice on mobile technology. You will be aware that modern mobiles or "smart phones" or mini tablet devices are in essence smaller faster personal computers and provide the same level of internet access with better connectivity and networks available today. 4G, we are assured, is just around the digital corner for us in Highland!

The latest smart phones provide great opportunities for being more connected in the digital world but can also therefore pose a risk for users to be identified or located, and send or receive images they may feel uncomfortable with. It's really important that we raise awareness and specifically highlight the dangers of young people finding themselves in uncomfortable or compromising situations.

Research recently conducted by the NSPCC has reported that in most cases where young people have been in situations of risk from being involved in transmission of inappropriate images, this has been through interaction with their peers rather than strangers. It is vital that modern technology is used with responsibility and regard for the personal safety and privacy of both the user and others both now and for the future. There are also implications for young people who may not know that they could be breaking the law by receiving or sending such images or footage. They also may be unaware that images may be circulated far and wide or uploaded without their permission or knowledge.

What can I do to keep my child safe?

We would ask you to think about the same kinds of risks you would talk about with your child if you had purchased a mini online computer with integrated webcam capable of video chat and video recording. Remind them of the future consequences of pictures, video clips or text messages that can be widely distributed without permission or knowledge only to resurface embarrassingly at a later date!

In purchasing a mobile phone or smaller tablet type device with network access, discuss firstly what your family boundaries might be, financially, App purchases, insurance, theft and appropriate usage. This also may include not sharing their number or email address with

strangers or posting it on social networking site profiles. To prevent unauthorised use it may be advisable to use a password pin to unlock the phone.

Many types of communication for speaking, texting or video-chatting can now work irrespective of phone signal or "credit" on a phone network. For example, Apple iPhones and iPads use a technology called Face Time or iMessage which allows users to interact based on account details or email rather than phone number. Many other apps freely available also provide this facility. As new popular games for phones allow the user to play anyone freely across the globe, it's vital that young people know how to keep safe and not disclose their name, location or personal identifiable information.

Keep lines of communication open with your child to ensure that they are not afraid to tell you if they have received an image, unwanted contact or are being pressurised to send any inappropriate photos of themselves. Remind them to report any images they receive to yourself or an adult they can trust.

Remind them to switch off the Bluetooth®, keeping this switched off keeps the device safe from receiving unsolicited images, videos or having their phone hacked.

Most modern mobiles (iPhones and Android Smart phones) have location settings which may be applied to functions of the phone or apps they use. This may mean that images they take either to keep or share might also contain details of where the user took that image, this information is then stored in the image identifying personal information. For advice on disabling location settings please check the phone instruction manual or contact your network provider.

Discuss with your child how to turn off location settings or ask when it may be appropriate to have this turned on. For example, some parents may wish, at certain times, for these settings to be kept switched on so that a young person could be located in emergency situations. Ask them to come up with their own ideas of situations.

Mobile phone and device theft is often opportunistic and it is wise to remind them that they should not leave their phone in full view unattended.

Remind them of street safety; it is important to be extra careful when walking, running, crossing roads or riding a bike whilst using music players on mobile phones, browsing the internet, chatting or texting.

Advice for parents and carers

As parents and carers we know it's often difficult during a lively busy household to find the time to sit and have a really good chat about things. The advice here is to keep talking to your child or children. Ask them what they like doing online… ask them to show you their favourite sites. Don't be afraid to ask them what concerns them too, things they see and do online and whether this is things they see (content on sites) things they do or others do or say (conduct) or communication from people they maybe don't want, this could be contact from people they know who are not friends or may be strangers. We more commonly call these the three Cs – Content Conduct and Contact.

Although it may be uncomfortable for some parents or carers, be prepared to talk about violent or sexualised content – research has recently shown us that this is what concerns children and young people the most. Make sure they know who they can speak to if they see, hear anything that concerns them. Be a good role model yourself; contribute to safer online communities by encouraging responsible use too and good use of technology. You can also ensure you have filters on your broadband or internet browsers to ensure that you do as much as you can to support them as they use devices at home. You can also suggest using safer child friendly search engines such as www.kidrex.org

Also please remember it's **never too late** to report any concerns, the professionals here in Highland an online are here to support. No-one is going to judge you or your child. Below are some top tips with a little supporting information.

Gaming

Games on consoles such as the Xbox, PlayStation, PC or Wii are now more than likely to be connected to the web, games can also be very educational too, and it's just a different form of play for many. Big multi-player games are incredibly popular and will only get more attractive in the future with gadgets and technology to make it seem more real and enhance the user experience. The same kinds of responsible behaviour need to be highlighted here; particularly not giving out personal information like location or full name to other players they meet online but do not know in the offline world. Also make sure that you child knows when to switch off and have a healthy balance to playing, learning and sleep! Think about age ratings too. For more information on ratings for games you can go to http://www.pegi.info/en/index/

Some top tips for children and young people to keep safe

Treat your passwords like your toothbrush. Never share and change them often!

This is a fun way to get children to think about their passwords. We know sometimes people have one password or phrase for all their accounts like eBay, Hotmail, Facebook or Twitter. If they shared their password or passphrase they might be letting someone have access to many more sites. We know sometimes children like to show they trust their friends by letting them have their password; we try to ensure that children and young people understand that they are protecting their friends by not giving them their password, it means they won't get blamed if it is hacked!

Make sure you know who people are before adding them as "friends".

This is a really important, especially for friends of friends, sometimes it's important to remember that not everyone is who they say they are. It's better to have a close group of friends rather than lots of friends just for the sake of it.

Know how to "block" people, though remember they might have different accounts!

Most social networking sites will give you the ability to block someone, but remember this doesn't necessarily work as it might only work by the email address of account of that person. Someone could create another account with a different name.

Don't post your personal information – full date of birth, email addresses, phone numbers and location on your profile, an update or tweet.

Explain that if someone had all these snippets of information that collectively they could provide enough information to steal your identity, they might be able to pretend to be you and when they are older maybe make a fake account in their name, take out a credit card or loan! Also explain that this kind of information being online might attract unwarranted email spam or unpleasant phone calls.

Know who to tell things to that concern you, talk to your parent, teacher or youth worker or use the CEOP Report Abuse Button.

This is really important; secrecy is a weapon that unpleasant people use to hurt other people. All children and young people should know who to speak to if they have any concerns. CEOP provides a great online button which in one click enables access to appropriate support, advice and reporting. This is available as an app or Facebook or Twitter or their main website www.thinkuknow.co.uk The important aspect here is that having the ability to talk about things in a safe, non-threatening, non-judgemental way helps to encourage children and young people to share their concerns.

NEVER meet up with anyone offline without your parent/carer or trusted adult.

Sometimes it's easy to build up trust with someone you haven't met before, either through gaming, social networking or chat room. But no matter how much you think you know someone and develop a friendship with them, you must never meet up with anyone without your parent, carer or trusted adult.

Don't rely on "privacy" settings to safeguard your personal information on your profile or posts.

Sometimes we hear that privacy settings will keep your information private, this is really a myth. You will be sharing your information with a group of friends, possibly even friends of friends and privacy settings can be very confusing! Others who may see your information can still share it and pass it on to others; we do not ask our friends to sign up to a confidentiality agreement. So it's really important to remember that even if your profile is set to private it is not a safeguard for your information or even bad behaviour!

Think before you post whether it's a picture, video clip or comment about yourself or others… it is going to be out of your control!

It's important to think about the content of images of film that you have uploaded or "liked" what does this say about you? It's also important to think about the future here as you are creating a digital "footprint" that is that these little snippets of information can paint a picture of you and can be found in the future.

Make sure you "log off" when you are finished.

Not only is it good to save the planet and log off and power down, it is important to log off so no-one can jump in your place and log in pretending to be you and cause mischief!

If it looks too good to be true, it probably is!

It is really easy to get taken in by hoaxes and scams, we've all had those emails where you have won something or a tax rebate is coming your way. The advice here is to never open anything suspicious or mail which is unexpected or unsolicited.

For more safety advice go to www.thinkuknow.co.uk

This is a great site for all – children and young people of ages, parents and carers and teachers. The Highland E-Safety Group also has its own website for e-safety advice: www.highlandesafety.wordpress.com

What should I do if I am concerned about a child?

Tell someone what your concerns are – speak to a teacher, a doctor, a social worker, a police officer or school nurse. Phone 01463 703488 for general enquiries email: CPAdmin@highland.gov.uk

For information on the work of the Highland child protection committee go to http://www.forhighlandschildren.org/2-childprotection/

About Louise Jones

Louise is the ICT curriculum liaison manager for the Highland Council education, culture and sport service and chair of the Highland E-Safety Group.

Louise is an ambassador for the Child Exploitation and Online Protection centre (CEOP) and has led on the e-safety work in Highland since 2008. Louise can be contacted on louise.jones@highland.gov.uk