Calderdale
Safeguarding
Children Board

HELPING CHILDREN AND YOUNG PEOPLE TO STAY SAFE ON-LINE

E-SAFETY GUIDANCE

February 2015

Contents

E-Safety Protocol

1. Introduction

This protocol has been produced to guide practitioners and volunteers working with children and young people in a range of settings; and fostercarers and residential staff caring for children and young people, to promote the e-safety of children and young people they are supporting.

Children and young people go online to connect with friends, and make new ones, to browse the internet for information, chat with others and play games.

They may:

- search for information or content on search engines like Google and Bing
- share images and watch videos through websites or mobile apps like Instagram, Pinterest, Vine and YouTube
- use social networking websites like Facebook and Twitter
- write or reply to messages on forums and message boards
- play games alone or with others through websites, apps or game consoles
- chat with other people through online games, BBM (Blackberry Messenger), game consoles, webcams, social networks and tools like Whatsapp

When online, children and young people can learn new things, get help with homework, express themselves creatively and connect with friends and family.

However, there are also risks.

2. Risks On-Line

Children and young people may be exposed to:

2.1 Inappropriate content, including pornography

Children and young people may see illegal or unsuitable content online, such as:

- pornography
- child abuse images
- dangerous advice encouraging eating disorders, self-harm or suicide
- excessive violence or race hate materials.

Some websites show illegal content. Others that are legal might have unregulated advice or are meant for adults only.

Children may come across this content by mistake, or they may look for it because they're curious. Promises of special offers or prizes can also draw young people in

2.2. Ignoring age restrictions

Some websites and games use age restrictions and checks to make sure that children don't see unsuitable content.

Children must be at least 13 to register on most social networking websites. But there's not a lot standing in the way of children joining at a younger age.

Age limits are there to keep children safe so adults should not feel pressurised into letting younger children join these websites

2.3. Communicating with people they don't know

Children and young people may chat or become 'friends' with people on social networks or online games, even if they don't know them or have never met them in person. In this context a ‘friend’ may be someone they have in real life, someone they have ‘met’ on-line or a friend of a friend. Making someone a friend on-line gives that person access to the information they have included on their profile, for example, interests, location, appearance. Children act differently on line to the way they act in the real world – it is easier to say, do and reveal things on-line when apparently hiding behind a computer

2.4. Grooming and sexual abuse

Grooming is when someone builds an emotional connection with a child to gain their trust for the purposes of sexual abuse or exploitation, Children and young people can be groomed online or in the real world, by a stranger or by someone they know - for example a family member, friend or professional.

Groomers may be male or female. They could be any age.

Many children and young people don't understand that they have been groomed, or that what has happened is abuse.

On-line groomers can use social media sites, instant messaging apps including teen dating apps, or online gaming platforms to connect with a young person or child.

They can spend time learning about a young person’s interests from their online profiles and then use this knowledge to help them build up a relationship.

It’s easy for groomers to hide their identity online - they may pretend to be a child and then chat and become ‘friends’ with children they are targeting.

Groomers may look for:

- usernames or comments that are flirtatious or have a sexual meaning
- public comments that suggest a child has low self-esteem or is vulnerable.

Groomers don’t always target a particular child. Sometimes they will send messages to hundreds of young people and wait to see who responds.

Groomers no longer need to meet children in real life to abuse them. Increasingly, groomers are sexually exploiting their victims by persuading them to take part in online sexual activity.

When sexual exploitation happens online, young people may be persuaded, or forced, to:

- send or post sexually explicit images of themselves
- take part in sexual activities via a webcam or smartphone
- have sexual conversations by text or online.

Abusers may threaten to send images, video or copies of conversations to the young person's friends and family unless they take part in other sexual activity.

Images or videos may continue to be shared long after the sexual abuse has stopped.

Children can be at risk of online abuse from people they know, as well as from strangers. Online abuse may be part of abuse that is taking place in the real world (for example bullying or grooming). Or it may be that the abuse only happens online (for example persuading children to take part in sexual activity online).

Children can feel like there is no escape from online abuse – abusers can contact them at any time of the day or night, the abuse can come into safe places like their bedrooms, and images and videos can be stored and shared with other people.

2.5. Bullying online or cyberbullying

Cyberbullying is an increasingly common form of bullying behaviour which happens on social networks and mobile phones. Cyberbullying can include spreading rumours about someone, or posting nasty or embarrassing messages, images or videos.

Children may know who's bullying them online – it may be an extension of offline peer bullying - or they may be targeted by someone using a fake or anonymous account. It’s easy to be anonymous online and this may increase the likelihood of engaging in bullying behaviour.

Cyberbullying includes:

- sending threatening or abusive text messages
- creating and sharing embarrassing images or videos
- 'trolling' - the sending of menacing or upsetting messages on social networks, chat rooms or online games
- excluding children from online games, activities or friendship groups
- setting up hate sites or groups about a particular child
- encouraging young people to self-harm
- voting for or against someone in an abusive poll

- creating fake accounts, hijacking or stealing online identities to embarrass a young person or cause trouble using their name
- sending explicit messages, also known as sexting
- pressuring children into sending sexual images or engaging in sexual conversations.

2.6. Sharing personal information

Privacy controls can limit who can see your child's details, like their name, age and where they live. But when a child connects to someone as a 'friend', that person will have access to the child's personal information.

Some 'free' games might ask the child to fill out lots of details before they can play and then illegally rent or sell this data on to others.

In order to prevent this from happening, there is a need to switch off or adjust settings using GPS or location tracking.

Many apps and social networking sites use software to locate where the user is. Children and young people can also reveal their location by tagging photos, such as on Instagram, or checking in on Facebook or Foursquare.

This means that people can find out where the child lives, socialises, works or studies.

2.7. Gambling or running up debts

Many online games are free but offer the chance to buy items such as extra lives or new levels. So children may run up big bills without realising.

Gambling sites have strict measures to make sure that their users are adults, but young people aged 18 and over could be enticed by offers and prizes on gambling websites and build up large debts.

2.8 Radicalisation

Some children and young people are being targeted, via social media sites, to promote and engage them in extremist views and in viewing content that glorifies violence. Research concludes that children and young people can be trusting and not necessarily appreciate bias that can lead to them being drawn into these groups and adopt extremist views, which, In some cases, influences and radicalises the young person so that extreme content is normalised.

Anyone who identifies that a child or young person may be vulnerable to being drawn into violent extremist activity, for example as a result of observed behaviour or reports of conversations to suggest the child supports terrorism and/or violent extremism, must report these concerns to the named or designated safeguarding professional in their organisation or agency,

2.9 Cyber Crime

The term cyber crime refers to a variety of crimes that are conducted online using the internet, including paedophilia, stalking, bullying, fraud, spam emails, viruses and hacking. These crimes allow the person to hide their identity and whereabouts. It also allows them to target someone directly through emails or viruses, or by hacking into their online accounts, home or work computers, mobile phones or other electronic devices.

Cyber crimes include: being sent obscene emails, bullying material or junk mail. Being tricked into sending money, personal details or identity. Intentionally contaminating a computer with viruses.

This sort of crime can lead recipients feeling scared, angry, fearful, sick, under siege, afraid to use a computer or the internet and unsure who to call for help.

2.10 Revenge Porn

Revenge porn is the act of publishing intimate photos, videos and contact information of a former boy or girlfriend on-line without their consent. The images may be captured with or without the subject’s knowledge. Sometimes the images are used to blackmail, cause emotional distress or discredit the person.

Private videos and photos can be leaked even after they have been deleted and sold to porn sites. Trolls spread the images of people they don’t know to embarrass them or ‘just for a laugh’. Some websites are set up to earn money from sharing revenge porn. Once the images are released on-line, it is often very difficult to take them down.

People sending intimate photos or videos without the subject’s consent can now be prosecuted.

3. Promoting the safety of children and young people on-line

In order to promote the safety of children and young people on-line, it is important to put safeguards in place to regulate and monitor the usage of the internet. This can include:

Talking to children and young people about their use of the internet, how to stay safe and what to do if they ever feel scared or uncomfortable.

Showing interest in how the child uses the internet and suggest they nominate a trusted adult to become their friend so that they can see their profile and what sites are being used and so they can let you know if they see anything worrying on the child's profile.

Agreeing some groundrules together depending on the child’s age and what is appropriate for them, for example

- the amount of time they can spend online
- when they can go online
- the websites they can visit or activities they can take part in
- sharing images and videos
- how to treat people online and not post anything they wouldn't say face-to-face.

If the child plays online games:

- check the age rating before they play
- make sure you know who they're playing with
- talk to them about what information is OK to share with other players
- negotiate the amount of time they spend playing online games.

Applying or suggesting parents/carers use parental controls on social networks, online games and browsers and on both hardware and software that can filter, restrict or monitor what the child can see.

Parental controls can be set up to stop the child from seeing unsuitable or harmful content online:

- Internet Service Providers (ISPs), such as Virgin Media, TalkTalk, Sky or BT, provide controls to help the adult filter or restrict content.
- Laptops, phones, tablets, game consoles and other devices that connect to the internet have settings to activate parental controls.
- Software packages are available - some for free - that can help you filter, restrict or monitor what the child can see online.

Remember that if the child goes online away from home, the same controls might not be in place at other people's houses or on public Wi-Fi. Agree with the child how they will use public Wi-Fi or let other parents know what the child is or isn't allowed to do online.

Levels of control can be changed as the child grows older. If removing the controls completely, make sure you agree what behaviour is acceptable online first.

Make sure the content the child sees is age appropriate. check that the websites, social networks and games they're using are suitable for them.

Check that the browser's homepage (the page that you see when you open an internet window) is set to a website that you're happy for the child to see.

Online games, movies and some websites will also have an age rating or minimum age to sign up. Age limits are there to keep children safe so you should not feel pressured into letting the child sign up or use websites that you feel are not suitable or they are too young for.

Check the child knows how to use privacy settings and reporting tools

Check the privacy settings on any online accounts your child has, like Facebook or games, and remind them to keep their personal information private.

Talk to the child about what to do if they see content or are contacted by someone that worries or upsets them. Make sure they know how to use tools to report abuse.

Appendix 1 provides an example of an ‘Acceptable Use Agreement’ that can be adapted or used with children and young people.

Most large organisations have ICT user agreements that set out the professional responsibilities and expectations of staff and volunteers who use electronic information systems to communicate with children and young people. Appendix 2 provides an example of an ‘ICT Acceptable Use Agreement’ that can be used or adapted for staff and volunteers.

4. Useful Websites

For more information on these and other related subjects, use the following links:

https://www.victimsupport.org.uk/help-victims/ive-been-affected/cyber-crime

http://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

http://www.childline.org.uk/explore/onlinesafety/pages/onlinesafety.aspx

http://www.thinkuknow.co.uk/

http://www.saferinternet.org.uk/advice-and-resources/young-people

http://www.barnardos.org.uk/what_we_do/who_we_are/resources_internet_safety.htm

http://www.wisekids.org.uk/online_safety_tips_kids.htm

http://www.ceop.police.uk/

http://www.safenetwork.org.uk/HELP_AND_ADVICE/Pages/safety_online.aspx

Appendix 1

E-Safety
‘Acceptable Use Agreement’ for Children and Young People

Child’s agreement

1.	I will not give out personal information such as my address, telephone number, parents’ work address/telephone number, or the name and location of my school without my parents’ permission.
2.	I will tell my parents right away if I come across any information that makes me feel uncomfortable.
3.	I will never agree to get together with someone I “meet” online without first checking with my parents. If my parents agree to the meeting, I will be sure that it is in a public place and bring my mother or father along.
4.	I will go online or play video games when my parents say it’s OK and limit my online time so that it doesn’t interfere with homework or other activities.
5.	I will not respond to any messages that are mean or in any way make me feel uncomfortable. It is not my fault if I get a message like that. If I do I will tell my parents right away.
6.	I will talk with my parents so that we can set up rules for going online. We will decide upon the time of day that I can be online, the length of time I can be online, and appropriate areas for me to visit. I will not access other areas or break these rules without their permission.
7.	I will not give out my Internet password to anyone (even my best friends) other than my parents.
8.	I will check with my parents before downloading or installing software or apps or doing anything that could possibly hurt our devices or jeopardise my family’s privacy.
9.	I will be a good online citizen and not do anything that hurts other people or is against the law.

10.	I will help my parents understand how to have fun and learn things online and teach them things about the Internet, computers and other technology.

I agree to the above

____
Child sign here

I will help my child follow this agreement and will allow reasonable use of the Internet as long as these rules and other family rules are followed.

____
Parent(s) sign here

Young person’s agreement

1. I will be respectful to myself and others. I won’t bully and won’t tolerate bullying by others.

2. I will be a good online friend and be supportive of my friends and others who might be in trouble or in need of help.

3. I won’t post or send pictures or other content that will embarrass me, get me into trouble or jeopardise my privacy or security.

4. I will respect other people’s privacy and be courteous when posting photos or other content about them.

5. I’ll be conscious of how much time I spend on the web, phone and other devices and won’t let use interfere with sleep, school work and face-to-face relationships.

6. If they need my help, I’ll assist my parents, teachers others in their use of technology.

7. I will respect other people’s digital property and space. I won’t steal, hack, break into anyone else’s accounts or use other’s content without permission.

8. I will protect my passwords and practice good Net security.

9. I will be thoughtful in my use of copy and paste. If I use anyone else’s content or images I will quote them, give them credit and link to them if appropriate.

10. I will help create a culture of respect and tolerance at my school and among my friends.

I agree to the above ____________________________ young person sign here

I will help my son/daughter follow this agreement and will allow reasonable use of the Internet as long as these rules and other family rules are followed.

____

Parent(s) sign here

Appendix 2

ICT 'Acceptable Use Agreement'
for Staff and Volunteers

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with children and young people, they are asked to sign this code of conduct. Members of staff and volunteers should consult [name of organisation's] policy for Internet access for further information and clarification.

- I understand that I must not use [name of organisation] ICT system to access inappropriate content

- I appreciate that ICT includes a wide range of systems, including mobile phones, digital cameras, email, social networking and gaming devices and that ICT use may also include personal ICT devices when used for business.

- I understand that my use of [name of organisation] information systems, Internet and email may be monitored and recorded to ensure policy compliance.

- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager. I will not use anyone's account except my own.

- I will not install any software or hardware without permission.

- I will ensure that personal data is stored securely and is used appropriately, whether on or off site. It must NOT be kept on removable storage devices.

- I will respect copyright and intellectual property rights.

- I understand use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

- I will report any incidents of concern regarding children's safety to [name of organisation's] e-Safety Coordinator, the Designated Child Protection Liaison Officer or Line Manager.

- I will ensure that electronic communications with children and young people including email, Instant Messaging and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.

- I will promote e-safety with [name of child or young person]s in my care and will help them to develop a responsible attitude to system use, communications and publishing.

- [name of organisation] may exercise its right to monitor the use of [name of organisation's] information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of [name of organisation]'s information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Staff and Volunteer Code of Conduct for ICT.

Signed: ……………………………… Capitals: …………………….. Date: ………

Accepted for [Name of Organisation] …………………………………………………..…

Capitals: ……………………………………….……… Date: ………………………..