DERBYSHIRE County Council

INTERNET SAFETY POLICY FOR ADOPTERS, FOSTER CARERS & STAFF IN CHILDREN'S HOMES

Introduction

Over the last few years, advances on the internet have changed completely in the way we communicate with each other, share and store information, expand our knowledge, go shopping, book holidays, and build and expand friendship networks.

For many parents and carers, the internet is still a novelty – for children growing up now, the internet is a fact of life and their lives will be increasingly 'web' based, whether on their personal computers, games consoles, mobile telephones, at home or at school. While the benefits it can offer, with regards education and learning are immeasurable, it can also pose risks and possible harm for young people. Derbyshire County Council believes that safe care and responsible internet use should not be 'self-taught' but, rather, that families and households work together in understanding the best way to stay safe online.

It is worth remembering that children in care, and adoptive children, are particularly vulnerable. They may be at risk from contact from friends or family members, when it might not be in their best interests to be contacted – there is a chance that revealing their care status could make them particularly exposed to inappropriate behaviour or grooming, or online bullying.

It is also worth remembering that carers, adopters and people who work with children in care can also be vulnerable; children in their care may want to contact family and friends on line – they may make allegations and accusations on line, they may, as a result of their backgrounds or previous home environments, participate in bullying and information they disclose online could compromise your role as a carer or adopter.

Staying Safe

Most young people would consider the internet a central part of their life; as they communicate – whether amongst their immediate friends, their school or as part of a much large social group. Unfortunately, what a person may say or do online, is not necessarily the same as what they would say to somebody's face; by sitting at a personal computer they are detached from the people they are communicating with and the internet can often be used negatively. The fact that harmful messages or contact can take place at any time, and within the home, also means that for many people who may be at risk online, there is no respite or refuge.

Essential Recommendations

- Personal information should never be given out or displayed online – age, gender, address, telephone numbers, passwords and PIN numbers. If you need to use personal details to purchase goods online, only use a trusted and secure website.

- 'Friends' you make online are strangers – you have never met them personally, and all you know about them is what they have chosen to tell you. We know that young people do meet people they have befriended on the internet. If a young person, in your household, wants to meet someone offline, it must be fully supervised by their parent or carer, in a public place or venue.

- Report any behaviour which you consider threatening, inappropriate, frightening or bullying. There are list of sites where you can report, in the appendix at the back.

As the internet changes, the basic principles of what young people go online for and the basic principles of staying safe remain almost unchanged. For the vast majority of children, participating online allows them to:

- Chat
- Message
- Network
- Game

Chat

Most people will be aware of 'chat rooms' – this is a site where large numbers of people can communicate simultaneously, in a form of online conference. Chat rooms can be 'standalone' or they can be a part of a wider site. Users are able to talk, swap information such as music files or images, build friendships and create virtual environments, similar to those found in console games.

As internet use widened, chat rooms, initially, attracted a great deal of criticism, as they were being seen as a means to groom children and young people and incidents of inappropriate and harmful behaviour, as a result of contact in chat were not uncommon. Since then, chat rooms have become increasingly moderated – either by employees or volunteers on the site, who remove or report offensive and suspicious activity or by filters in the programs which are triggered by specific words or phrases.

Safe Chat

- Awareness – the best way to ensure safe care online, is to be as informed as possible about sites that children like to use. We don't expect parents and carers to become computer experts, but it is helpful if you speak to the young people in your home and understand what they are getting out of the internet.

- Young people find using chat rooms and messaging an easier way to express their feelings. Advise children in your home not to reveal personal information or email addresses with people they have not met in real life. Many chat sites, aimed at teenagers, are specifically aimed at dating and finding relationships and you should consider whether it is appropriate that the children in your home should access them.

- Language – chat users will abbreviate and shorten words to make it quicker to communicate, much like texting ('A/S/L' – Age, Sex, Location, 'POS' – Parent over shoulder, 'LOL' – Laugh out loud). This can be confusing but sites such as Thinkuknow (https://www.thinkuknow.co.uk/) have glossaries of chat speak.

Messaging

Instant Messaging, or IM, is a form of simultaneous 'chat' – unlike chat rooms, where users are able to speak to strangers in a shared spaced, instant messaging takes place between people who possess each other's phone numbers or social networking site friends lists, as a user receives more 'friends', they can increase the size of their network and, with the default settings on all IM providers, it is extremely easy to add new friends to a chat network. Unlike chat rooms, IM is not moderated.

Safe Messaging

- Address lists – many young people will be very competitive in expanding their friends lists, adding as many friends as possible. Email addresses and phone numbers can be traded and young people may not discriminate as to who they add to their contacts. This can lead to them allowing people into their networks, who may be looking to harm, bully or inappropriately contact vulnerable young people.

- Moderation – although moderators in chat rooms and forums do not have to undergo checks, as a carer or adopter would, they still offer some form of protection against offensive or threatening behaviour. IM is not moderated and so users should be especially careful at to what information they reveal, even amongst people they consider 'friends'.

- Bullying – Instant Messaging can be used to bully and intimidate. Threats, name calling, offensive or altered images can be shared very quickly and easily across friend networks.

- Personal contact – Instant Messaging enables users to communicate directly through mobile phones or webcams. They also allow for very fast and easy-to- use photograph and file sharing. The implications are that young people could risk compromising themselves by sending images, or having screen images 'captured' and that by sharing images, even with friends, they no longer have any control over them.

Social Networking Sites (SNS)

Social Networking Sites (SNS) such as Facebook, Instagram and Snap Chat are websites which allow users to build networks of friends, through shared interests, and can then be expanded with addition of mutual friends.

SNS are one of the fastest growing phenomena on the internet, and, at the time of writing, sites such as Facebook currently have over 2.38 Billion users in 2019. They present many of the risks associated with chat rooms and instant messaging, but they also pose problems that are unique to Social Networking. Any contact within an SNS is not moderated and, although age restrictions apply to virtually all sites, these can be easily over ridden and are not compulsory.

With regards fostering and adoption, there are concerns around contact and allegations – increasingly, there are incidents where adopted children and children in care are using SNS to directly contact parents and birth relatives and to post accusations and allegations against their carers or adopters. Similarly, carers have disclosed confidential information and revealed the identity of children in their household.

Safe Social Networking

- As with IM and Chat Rooms, SNS create the chance for inappropriate behaviour and contact.

- Privacy – SNS default settings allow users to place a large amount of personal information (telephone numbers, home and work addresses, email addresses) in the public domain on their profile page. Carers and parents, and the children they care for, should check the privacy settings of the site they are using to ensure that their contact details are hidden.

- Bullying – SNS allow bullies the opportunity to rapidly disseminate threats, intimidating messages, images and accusations across a very large number of people, in a very short space of time.

- Control – Social Networking lets users create, potentially, constantly growing networks of friends, through connecting with mutual friends or with people who share the same interests. This can mean that posts, photographs and shared messages can be seen and read by people outside your friends list.

- Inappropriate and Illegal Behaviour – many Social Networking Sites allow members to form and join online groups who promote or condone illegal activity (car cruising, substance misuse, football violence, possess racist or homophobic views), which would be unsuitable for both carers and parents and children in care, within Derbyshire County Council.

Gaming

For many young people, online and console gaming is the most popular way of spending their free time, combining both the opportunity to play games whilst interacting with other gamers, either within their own friends' network or across the world. Online gaming takes two forms; either through web based games or through games consoles, such as the XBOX 360 or PlayStation 3. Games such as Fortnite and Minecraft offer 'real time' gaming, where players can interact with each other to complete missions or tasks, in pursuit of virtual rewards, and many respects, players would communicate much as they would through a chat room, with similar levels of moderation. In the last few years, console games have expanded rapidly into the online gaming market to that extent that most new games now are solely for online use.

Safe Gaming

- Time – one of the main issues concerning online gaming, is the amount of time that players spend online. As many consoles and personal computers are kept in bedrooms, and so effectively unsupervised, there is a risk that time spent gaming could encroach on school work, family time and socialising.

- Age Appropriateness – many games now are aimed at an adult market, with strong language, sexual content, violence or references to substance misuse and criminal activity. Games are given age ratings, similar to DVD's and carers and parents should ensure that children in their household are not exposed to content unsuitable for their age group and abilities. All consoles now have parental controls, which can be password set to limit time spent playing, the types of game played and the online contact list of the user.

- Inappropriate Behaviour – as with Instant Messaging, people can play online with friends or in open forums, with strangers. Incidents of abusive language, threats, intimidation and bullying are not uncommon. There have also been occasions where young people have been contacted through online games, as part of a grooming process.

Mobile Telephones

With improvements in technology, a far wider range of tariffs available to consumers and internet access available on the vast majority of mobile telephones, it is now both easy and relatively cheap, for people to use their phone much as they would a personal computer or tablet. The increase of internet enabled phones, combined with the fact that virtually all phones now have cameras and video, has created a number of concerns:

- Internet Access – it is possible now for young people to have instant, unsupervised access to the internet from their mobile handset.

- Photographs and Videos – the rise of camera phones has led to new trends, namely 'happy slapping', where incidents of violence or abuse are recorded and then broadcast and 'sexting', where users will record and send indecent images or sexually explicit text messages. Just as images shared online are beyond their owners control once sent, so too are those taken and shared from a mobile telephone.

- Bullying – mobile telephones have long been a way of intimidating, threatening or harassing people. 'Pay as you go' SIM cards are now so cheap and freely available means that it is possible for the bully to remain anonymous.

What Carers and Adoptive Parents Should Know

The fastest growing online community now, especially with regards Social Networking Sites, are not children and teenagers but adults, especially amongst adults aged from 35 to 50. Most of Derbyshire County Council's carers and adoptive parents will have some form of presence now on the internet, through membership of SNS or online groups and forums. As an authority, we believe that a level of safe care must be exercised to ensure not only the wellbeing of the child in your care, but also that of you and your own household.

- Confidentiality – we would advise you not to reveal or broadcast your status as a carer or an adopter. Such information can reach a large number of people very rapidly and, once broadcast, is beyond your control.

- Inappropriate Contact – it is recommended that children in your care do not reveal their names or any personal details online; use nicknames instead and don't post up photographs. If you need to use an avatar (an image which illustrates your profile), use a cartoon or non-related image. If carers are storing photographs online, use the privacy settings to prevent them being accessed, unless by people approved to do so - do not keep school photographs or any which might indicate where the child may be based.

- Allegations and Accusations - Report! If you, or a member of your household, have allegations made against you, which are circulated across the internet, report them immediately and do it as soon as possible; the longer an accusation or untruth stays on the internet, the more widely it can spread.

Safe Care – Practical Considerations

- Keep computers and, where possible, games consoles in open spaces or shared family areas.

- Set limits for the amount of time a young person can go online.

- Understand what sites children and young people like to use – ask them about what they explain what they enjoy about the internet and how the sites work.

- If you have a games console in your house – read the instructions. Parental controls and filters are very straightforward to use and Microsoft, Nintendo and Sony have excellent, easy to understand websites offering support and guidance.

- Speak to your supervising social worker if you have any concerns or suspicions about the child you care for, which might relate to their use of the internet; mood swings, irritable behaviour, unwilling to socialise or share information, are withdrawn or possibly aggressive.

Safe Care – Reporting Abuse

- CEOPS (Child Exploitation Online Protection Service). https://www.ceop.police.uk/ceop-reporting/

- Their partner Thinkuknow (https://www.thinkuknow.co.uk/), offers a wide range of support for parents and carers, and children and young people – it has updates and developments on internet misuse, teaching aids and educational videos and, most importantly, a reporting facility

This button, found on the Thinkuknow site, and also on sites who have agreed to sign up to CEOPS reporting facility allows users to immediately report abuse. If you or the child in your household has any concerns, click the button – choose from a list of issues (cyberbullying, hacking accounts, viruses, mobile telephones, harmful content, sexual behaviour) – it will then offer both advice around the issue and, if necessary, an option to report the incident to CEOPS with further support (such as Childline) available, if necessary.

It suggests instead that users maintain their privacy settings, in order to self-regulate posts and content. It is worth remembering that a parent or carer has no legal rights to the content of their child or foster child's site and Facebook will not intervene on your behalf.

It is recommended that if you do have concerns over Facebook content, report not only to Facebook but also to CEOPS, by sending them a link or screen grab of the page.

- Mobile Telephones. All UK mobile phone companies have facilities to deal with nuisance calls. If a user is receiving nuisance calls or texts, they can change that person's number and, with the involvement of the police, block the person making the calls.

- Games Consoles. The three leading console manufacturers, Microsoft (XBOX 360), Sony (Playstation) and Nintendo (Wii) all offer advice and guidance on safe gaming, setting parental controls, a reporting facility and regular updates. A list of links can be found in the final section.

- Make a note of which site you were using, and record the full address for any reporting – the best way to do this is via a 'screen grab', which will record exactly what is showing on your screen at that time. To do this, press 'Print Screen' or 'PrtScr' on your keyboard. This will automatically store your current screen display. Go to 'Word', click 'Edit' and then 'Paste' – this will then show your screen display as an image – click 'Save'

Maintaining Privacy

The most popular Social Networking Sites are, by far, Facebook, Instagram & Snapchat. They are at first glance, very easy to use and its search facility makes it very easy to find people to add as 'friends'. If, however, you wish to keep your details private and limit the amount of information that is made available it is soon apparent that its privacy settings can be unwieldy and complicated.
The following are steps to show you how to set up basic privacy levels, which you can then fine tune as necessary;

- **Friends Lists**. This is the most important factor in staying safe. You can decide which friends see what information you post or have posted on your profile. If you post a photograph that you only want certain friends to see, restrict it to just that particular friends group. *If you leave your privacy settings unchecked, the default setting will be 'Everyone' – that means everyone in the 2.83 Billion Facebook network and anyone who might search for your details using Google.*

- **Remove Yourself From Search Results.** There may well be people who you might not want to find you, on Facebook. To stay hidden, go to the '**Search Privacy Settings**' page – click '**Edit Settings**' and enter your password – where it says '**Facebook Search Results**', select '**Only Friends**'. You will now no longer show on any Facebook searches.

- **Remove Yourself From Google.** It is very easy to search for people on Social Networking Sites just by typing in their full name – doing this on Google or other search engines, will show their photograph, interests and a list of friends. Again, you might prefer to remain on hidden from Google searches. To stay hidden, go to the '**Search Privacy Settings**' page – untick the box next to '**Public Search Results**', which says '**Allow Indexing**'. You will now no longer show on any Google searches (this may take a few days, whilst search engines delete previous information).

- **Photo Tagging.** You might not want either yourself, or a member of your household, tagged in a photograph.

  Go to the '**Profile Privacy Settings**' page – go to '**Photos and Videos of Me**'. Click on the drop down selector and click '**Custom**' option. Select '**Only Me**'. Only you will be able to see any picture you have been tagged in.

  If you want friends in your network to see the image, but not everyone, you can choose allowing one of your Friends lists or you can choose to remove people individually by going to '**Hide this from**' setting at the foot of the page.

- **Protecting Photograph Albums.** Facebook and Instagram offer a great deal of space to store photographs offline. Again, it is worth considering who you want to view your photographs – go to the '**Photos Privacy Settings**' and select the amount of access you want each album to have, by choosing from the '**Who Can See This**' box. It is now possible to individually choose which photographs are visible to which individuals or groups of friends, by selecting from the box.

- **Status and Relationships.** Changes in your relationships can be broadcast across your contacts list, as a news feed item. To keep your relationship private, go to your '**Profile Privacy Settings**' page and change the '**Family and Relationship**' setting to '**Only Me**'. This will block users from seeing your relationship status.

- **Making Contact Information Private.** If you do post personal information on your profile page (email address, telephone numbers etc.), you can limit who can see those details. Go to the '**Contact Privacy Settings**' page; here you can customise which of your Friends lists can see this information and, if needs be, hide it from as many individuals or Friends lists as required.

- You can set it more thoroughly by going to your Profile page. Click '**Info**' and go down to the '**Contact Information**' section – click '**Edit**' and padlock icons will show next to each piece of information (Emails, Screen Names, Mobile Phone, Address etc). Click on the padlock and a box will then show, '**Who Can See This?**' which will allow you to choose who sees your personal details.

- **Wall Posts.** While you cannot control what someone posts on their own wall, you do have some control over what is posted by a third party on your own. Go to your '**Profile Page**' – click on the '**Options**' button in the right hand corner of your Wall Publisher. This gives you steps to controlling what is posted on your Wall; '**Friends may post to my wall**' – unchecking this box, will prevent anyone communicating with you publicly. Or, click on the drop down box next to where it says '**Who can see posts made by my friends?**' and choose which Friends lists or individuals can view posts made public on your wall.

Guidance for Residential and Field Workers

Workers, caring for young people in Residential Units, face a number of issues unique to their situation. Derbyshire County Council believes that proper safe care, online, should be exercised by children and also the staff who care for them and special consideration should be exercised, with regards internet use.

There will be a temptation for children in care to contact Residential care and field workers online and make friend requests, through Facebook or similar sites. The authority does not condone members of staff befriending service users through social networking sites. We would not expect a teacher to befriend a pupil online and we feel that for a social worker to befriend a child in care, would be similarly inappropriate.

There is a possibility that a worker could be exposed to having allegations or accusations made online – it could also make them aware of aspects of the young person's social life which may not be in their best interests, and so compromise their professional relationship with that child.

If a worker has made or received contact with a young person, either through text or electronically, that conversation or message must be recorded on Mosaic.

If a young person is already a member of a social networking site there may be cases where we would advise some people (for example, a foster carer) to add the child to their own Facebook friends, using a restricted 'one to one' friends group, whilst in their care. Upon leaving their care, that friend should be removed – this creates a degree of monitoring for the carer, much as it would for a parent with their own children.

We would also remind all staff members to exercise a degree of caution, with regards comments made to their friends, on social networking sites. Views and opinions posted onto a 'wall' or via an electronic forum are not confidential and once posted, beyond the control of the person responsible. Recent, highly publicised examples in the media have shown that disparaging or harmful comments, or disclosures of confidential information, can lead to disciplinary action and/or legal proceedings.

Reporting and Support Links

- CEOPS & Think U Know Reporting sites
- https://www.ceop.police.uk/ceop-reporting/
- www.thinkuknow.co.uk

- Facebook – Click 'Report' located throughout the site or email abuse@facebook.com and use the CEOPS button

- Youtube – Click on 'Flag Content as Inappropriate' under the video box. You will need to create an account first, to access this service
- Record evidence. If moderators are present on the site, report any inappropriate behaviour or activity.

Games Consoles

- Playstation 3, http://www.ps-playsafeonline.com

- Xbox 360, https://www.xbox.com/en-US/live/abuse/

- Nintendo wii, http://www.nintendo.com/corp/parents.jsp