

Internet Safety

Policy no	Version	Date	Review frequency	Next review date	Policy owner
P (OP3)	1	April 2017	Annually	April 2018	L.Graham/ S.Davies

Table of Contents

Section		Page
1	Index	1
2	Policy Statement	2
3	Introduction	2
4	Staying Safe	3
5	Essential Recommendations- Chat	3
6	Messaging	4
7	Social Networking	5
8	Gaming	6
9	Mobile Phones	6

Name	Lena Graham/ Sarah Davies	Signature	
Designation	Registered Person/ Head of Care	Date	

Internet Safety

Policy Statement: The Children's Homes (England) Regulations 2015

'The protection of children standard 12.-(1) The protection of children standard is that children are protected from harm and enabled to keep themselves safe.'

1. Introduction

Advances on the internet have changed completely the way we communicate with each other, share and store information, expand our knowledge, go shopping, book holidays, and build on 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 regard to education and learning are immeasurable, it can also pose risks and possible harm for young people. We would not expect a young person to cross the road without knowing the 'Green Cross Code' first and Our Place Schools believes that safe care and responsible internet use should not be 'self-taught' but, rather, that that families and households work together in understanding the best way to stay safe online.

It is valuable to remember they children in care are particularly vulnerable. They may be at risk from contact from friends or family members, when it may not be in their best interest- 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 who work with children in care can also be vulnerable; children in their care may want to contact friends and family 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.

2. Staying Safe

Most young people would consider the internet a central part of their life; as pupils, as consumers and above all else as a means of communication- whether amongst their immediate friends, their family or as part of a much larger 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 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 young people do meet people they have befriended on the internet; A CEOP: Child Exploitation & Online Protection Centre survey in 2007, found that 25% had met someone they had first met online. - 25% of these children did so on their own. Of those that took someone with them, 83% took a friend rather than a trusted adult. If a young person using ‘Our Place Schools’ services wants to meet someone offline, it must be agreed and authorised by the placing authority, parents if appropriate, Registered Person and be risk assessed. The meeting must be fully supervised by appropriate parents or Our Place Schools staff prior to taking place and be held in a public place or venue.
- Report any behaviour which you consider threatening, inappropriate, frightening or bullying. There are lists 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

3.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 part of a wider site (chat rooms or forums are found on sites for football supporters, music or bands, or with shared interests and hobbies). 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 (such as Minecraft and Tierra)

As internet use widened, chat rooms, initially attracted a great deal of criticism, as they were 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 of the site, who remove or report offensive and suspicious activity or by filters in the programme 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 Our Place Schools staff or parents to be computer experts, but it is helpful to speak to young people in the 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 the 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 Our Place Schools will consider the appropriateness of access to these sites only where this has been identified within the young person's placement plan.
- 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 (www.thinkuknow.com) have glossaries of chat speak.

4. 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 space, instant messaging takes place between people who possess each other's email addresses and so create 'buddy lists'; as a user receives more emails, they can increase the size of their buddy network and, with the default settings on all IM providers, it is extremely easy to add new addresses to a chat network. The most popular IM systems are MSN Messaging (frequently abbreviated to 'MSN' - 'I've just been MSN'ing my friends'), AOL Instant Messaging (AIM) or Yahoo Messenger. Unlike chat rooms, IM is not moderated.

Safe Messaging

- Address lists- many young people can be competitive in expanding their buddy lists, adding as many friends as possible. Email addresses 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 do not have to undergo checks, as care staff do, they still offer some form of protection against offensive or threatening behaviour. IM is not moderated and so users should be especially careful as 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 friends networks.
- Personal contact- Instant Messaging enables users to communicate directly through microphones 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.

5. Social Networking

Social networking sites (SNS) such as Facebook, Bebo and My Space are websites which allow users to build networks of friends, through shared interests, they can then be expanded with an additional of mutual friends. Whilst these sites started as a way for students and graduates to stay in touch, they have since developed into providing platforms for members to express opinions and views, play games, share personal information, files, videos, music, store and display photographs and maintain online diaries (‘Blogs’).

SNS are one of the fastest growing phenomena on the internet, and in 2010 such sites as Facebook had over 410 million users. 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 a SNS is not moderated and, although age restrictions apply to virtually all sites, these can be easily over ridden and are not compulsory.

With regard to residential care there are concerns around contact and allegations- increasingly there are incidents of children in care using SNS to contact parents and relatives where this is not in their best interest to or agreed within the care plan to post accusations and allegations against their carers. Similarly carers have disclosed confidential information and revealed the identity of children in care homes.

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 being cared for should check the privacy settings of the site they are using to ensure that their contact details are hidden.
- Bullying- SNS allows bullies and 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 of children in care within Our Place Schools.

6. 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 such as World of Warcraft and Envoy, or through games consoles, such as the XBOX 360 or PlayStation. Sites such as World of Warcraft offer 'real time gaming, where players can interact with each other to complete missions or tasks, in pursuit of virtual rewards, and in 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 the 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 computers are kept in bedrooms, and so effectively unsupervised, there is a risk that time spent gaming could encroach on school work, family time, exercise 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 care 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.

7. 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. 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. That 'pay as you go' SIM cards are now so cheap and freely available means that it is possible for the bully to remain anonymous.

8. What carers should know

The fastest growing online community now, especially with regards social networking sites, is not children and teenagers but adults, especially amongst adults aged from 35 to 50. Most carers and adoptive parents will have some form of presence now on the internet, through membership of SNS or online groups and forums. As a service, we believe that a level of safe care must be exercised to ensure not only the well-being of the child in your care but also that of you and your household.

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

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. The final pages of this policy provides a comprehensive reporting procedure but carers are advised to do it as soon as possible, the longer an accusation or untruths stays on the Internet the more widely it can spread.

7. Use of computers and other devises

Our Place provides computer access for its children in the school and home. Children can have access to email, internet and webcam facilities.

School Use

The classrooms and Tech. room have computers for use during lesson time to assist with work and for ICT lessons. Children will have access to a wide range of computer programmes designed for the learning development. New learning programmes are constantly being researched to use with the children. In school the Tech room computer has internet access, with a 'nanny service' to protect children from unacceptable material and contacts.

Home Use

At all times the children's use of the internet will be monitored to protect them from unsuitable contacts. The internet access will have a 'nanny' service and parental blocking systems in operation.

Our Place and its entire staff shall observe all external laws and regulations, which are relevant to Information Systems. These include:-

Data Protection Act 1998
Copyright, Designs and Patents Act 1988
Computer Misuse Act 1990
Health and Safety at Work Act 1974

A breach of information security includes failure to comply with recognised standards of work relating to the use of information systems as set out in this Policy.

Breaches of information security will be treated very seriously and may be the subject of disciplinary action under Our Place's Disciplinary Procedures.

Breaches of any laws relating to the use of information and/or computers could, in some circumstances, be regarded as Gross Misconduct, the consequence of which is normally Summary Dismissal; that is, dismissal without notice or payment in lieu of notice.

ICT equipment, including parts of computers such as modems and network cards, must not be taken off site by staff without formal authorisation from the Senior Management Team.

If a terminal is to be left unused for a significant length of time, e.g. overnight and at weekends, always physically switch it off.

Computer equipment can be left switched on when not attended for either short periods or for overnight processing, etc. In these circumstances, every use should be made of the appropriate security features and of the power save features offered by the equipment in question.

When accessing the internet on Our Place resources, all staff must make sure that children comply with the following:-

Do not infringe copyright by using shareware software beyond its initial temporary licence period.

Do not use any internet facility to place an official order for goods or services unless authorised by the Key Worker or Senior Management Team.

Do not access web sites which are of a salacious or pornographic nature. Details of attempted access to all sites are recorded and regularly audited. Deliberately allowing a child to access sites of this nature will be treated as gross misconduct and handled according to Our Place's disciplinary procedures.

Do not access chat rooms or social networking

If left un-supervised at any time then a check of the browsers history must be done by the allocated staff.

Also the DSL's to check browsers history on a weekly basis and record this in the children Daily Diary.

If anything is found to be inappropriate or safeguarding concern then it must be reported to management with delay.

Young people are able to access Skype to enable face to face communication with family. A member of staff will support the young person at all times, staff will contact the family member prior to Skype conversations to take place to verify the conversation.